DOI 10.36622/VSTU.2022.25.4.001
УДК 004.056

МАТРИЧНАЯ ФОРМАЛИЗАЦИЯ ЦЕЛЕПОЛАГАНИЯ И РЕЗУЛЬТАТИВНОСТИ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ ЗАЩИТЫ ИНФОРМАЦИИ И ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Г.А. Остапенко, В.И. Белоножкин, Н.И. Баранников, А.А. Остапенко, А.Г. Краснобородкин, Т.Ю. Мирошниченко

Работа посвящена актуальной проблеме формализации целей, задач и ожидаемых результатов проектной деятельности при создании информационно защищенных систем. В этой связи предлагается построение матрицы целеполагания и результативности проекта, в которой столбцы относятся к выявленным на предварительном этапе противоречиям, задачам разрешения этих противоречий, ожидаемым результатам решения поставленных задач, их характеристикам новизны, практической и теоретической значимости. В свою очередь каждая строка матрицы ориентирована на конкретную задачу проектирования. Обобщенно целеполагание опирается на планируемые характеристики шанса полезности и риска ущербности создаваемой системы, для которых предлагаются аналитические метрики защищенности и формализуется поле проектной деятельности. Приводятся примеры построения необходимых формализмов для систем обеспечения информационной безопасности, а также – методик расчета рисков.

Ключевые слова: матрица, формализация, целеполагание, результативность, проектная деятельность, защита информации, информационная безопасность.

Введение

Целеполагание при проектировании всякой защищаемой (иные сегодня неактуальны) информационной системы (ИС) объективно базируется на двух характеристиках: шанс и риск. Первая является ожиданием в получении пользы от ИС, а вторая характеризует возможности нанесения ИС ущерба. Если пользу и ущерб в их значениях привести к некоторой общей оси условных единиц, то ситуацию в проектировании защищаемой ИС можно проиллюстрировать рис. 1, а, где приведены кривые плотности вероятности достижения значений пользы и ущерба f(v) и f(u), а также обозначены их матожидания M(v) и M(u). При этом пары вероятностей P(v) и P(u) наступления v и u образуют характеристики риска Risk [P(u), u] и шанса Chans [P(v), v].

Далее рассмотрим проектные ситуации, возникающие в ходе создания защищаемых ИС. Зачастую проектировщик независимо рассматривает M(v) и M(u), однако при совместном проектировании ИС и ее подсистемы защиты такой подход недопустим. Дело в том, что ослабленная защита, как правило открывает возможности для повышения производительности проектируемой системы (рис. 1, в). И наоборот, (рис. 1, б) усиление защиты зачастую приводит к снижению полезности. Аналитически эти проектные ситуации иллюстрируют следующие выражения:

$$M(u)\uparrow \Rightarrow M(v)\uparrow \text{ и } M(u)\downarrow \Rightarrow M(v)\downarrow. \quad (1)$$

Описанные выше эффекты довольно часто требуют количественной оценки. Для этого можно предложить метрику, где разность матожиданий нормирует по их полусумме

$$З = \frac{M(v) - M(u)}{\left((M(v) + M(u))/_2\right)} = 2\,\frac{1-\delta}{1+\delta}, \quad (2)$$

где $\delta = \frac{M(u)}{M(v)}$ – отношение матожиданий ущерба и пользы.

Предложенная метрика (1) может рассматриваться как степень защищенности проектируемой системы.

В тех случаях, когда корреляция матожиданий (1) не высока, мы получаем поле проектной деятельности, проиллюстрированное на рис. 2. Практические рекомендации освоения этого поля можно встретить в монографиях [1-7].

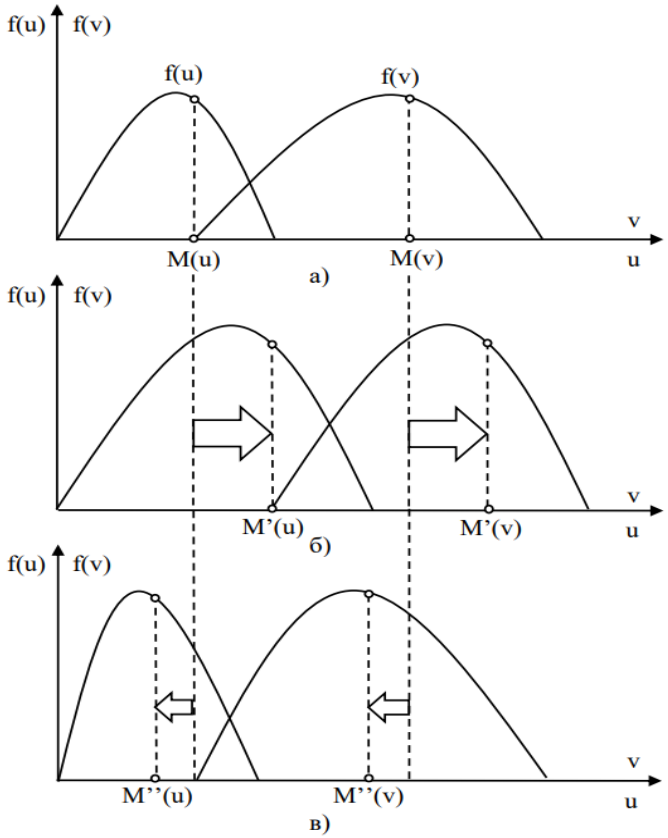

Рис. 1. Проектные ситуации для риска и шанса

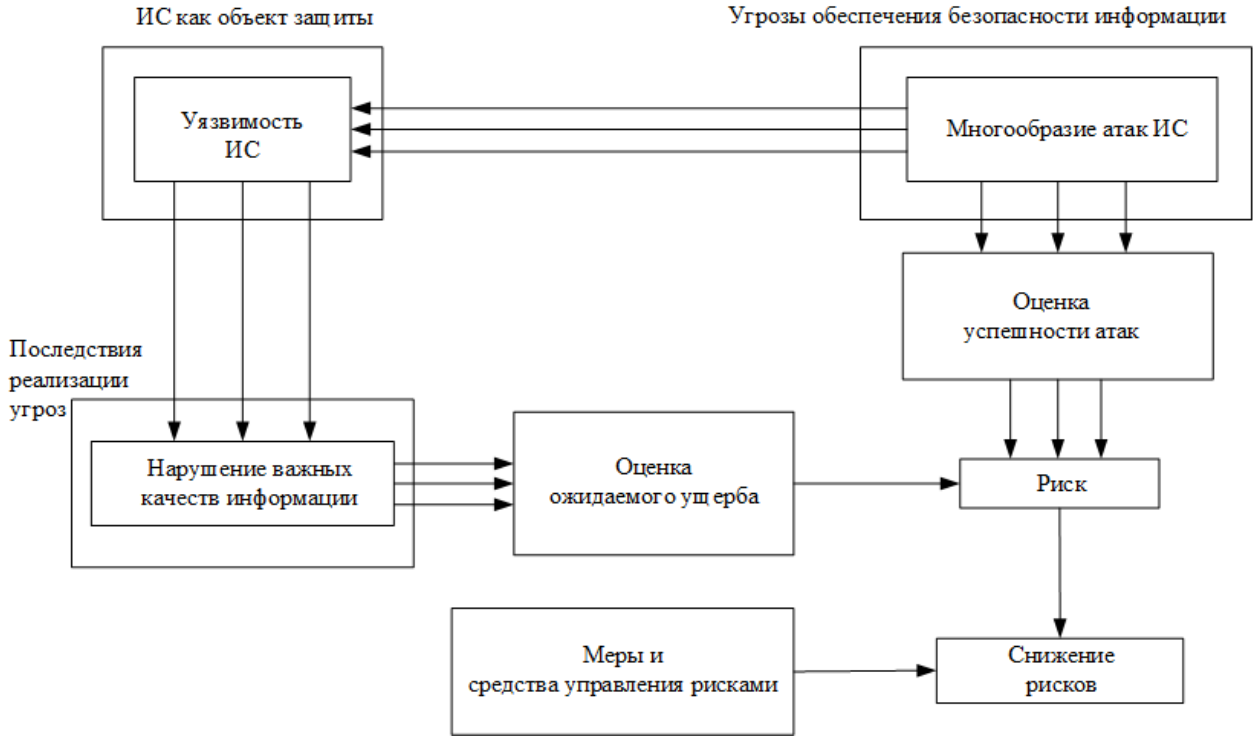

Рис.2. Поле проектной деятельности в сфере защиты информации и обеспечения информационной безопасности ИС

Объектом проектирования в данном случае выступает система (пространство и т. п.), подвергающаяся угрозам и/или атакам (конкретной разновидности), нарушающим безопасность (целостность, доступность и др.) информации.

Предметом проектирования являются исследование и управление процессами нарушения безопасности информации при реализации угроз (атак) заданного типа в отношении объекта проектирования.

Целью проектирования является разработка ИС с заданными функционалом и уровнем защищенности от определенных угроз за счет создания необходимых и достаточных обеспечений (правового, организационного, технического и др.), через оценку и регулирование рисков.

Предлагаемые шаблоны формализации целеполагания могут быть полезны при выполнении курсовых и дипломных работ студентами, а также при написании научно-квалификационных работ аспирантами.

Матричный подход к формализации целеполагания и результативности проектной деятельности

Технология формализации представлена в табл. 1, где строки матрицы определяют триаду противоречие-задача-результат и её характеристики, которые и образуют соответствующие столбцы. Взаимно однозначное соответствие (по строкам) обеспечивает полную определенность результатов проектной деятельности. При этом решаемые задачи определяют те противоречия, которые вскрыл (и счел наиболее значимыми) проектант. Четкость формулировок в элементах матрицы (табл.1) является обязательным требованием формализации. В противном случае процесс проектирования утонет в толковании разночтений и цель будет не достигнута.

В качестве иллюстрации рассмотрим процесс проектирования автоматизированной информационной системы, выявляющей источники деструктивного контента (ДК) в социальной сети (АИСДК).

Таблица 1

Матрица формализации целеполагания и результативности проектной деятельности

Анализ предметной области и выявление противоречий между сложившейся практикой и новыми требованиями к АИС с целью её дальнейшего совершенствования	Постановка задач разрешения каждого из выявленных и признанных существенных противоречий	Планируемые результаты решения поставленных задач в виде моделей, классификаций, алгоритмов, модулей, данных и т.п.	Ожидаемое повышение качества результатов в сравнении с аналогами проектируемой системы	Вероятные области эффективного использования планируемых результатов на практике	Возможные сценарии развития теоретической составляющей планируемых результатов проектирования
Первое противоречие	Поставленная для разрешения первого противоречия задача	Планируемый результат разрешения первого противоречия	Новизна планируемого разрешения первого противоречия	Практическая ценность планируемого решения первой задачи противоречия	Теоретическая значимость планируемого решения первой задачи
. . .	. . .	. . .	. . .	. . .	. . .
n-ое выявленное в аналогах противоречие	Поставленная для разрешения n-го противоречия задача	Планируемый результат разрешения n-го противоречия	Новизна планируемого разрешения n-го противоречия	Практическая ценность планируемого решения n-ой задачи противоречия	Теоретическая значимость планируемого решения n-ой задачи

Опираясь на анализ аналогов (при их наличии), или на требования предметной области при отсутствии систем-аналогов, можно выделить следующие требования (противоречия), которые будут разрешаться в данном проекте между:

1. Объективной потребностью выявления генераторов противоправных контентов и отсутствием таких средств в отношении соцсети ВКонтакте в виде автоматизированной информационной системы (АИС).

2. Насущной необходимостью сбора, хранения и анализа данных об источниках, генерирующих противоправные контенты в соцсети ВКонтакте, и отсутствии такой автоматизированной базы.

3. Отсутствие формализованных рекомендаций по противодействию вышеуказанным деструктивам.

Объектом исследования является социальная сеть «ВКонтакте», в которой генерируется и распространяется ДК, представляющий угрозу безопасности Российской Федерации.

Предметом исследования является выявление и риск-анализ ресурсов соцсети «ВКонтакте», генерирующей противоправные контенты: в социальных сети в целом и ее сообществах, через отдельно взятых пользователей, рассылку информационных сообщений, внешние узлы и гиперссылки.

Целью исследования является повышение защищенности пользователей социальной сети «ВКонтакте» за счет создания автоматизированной информационной системы выявления ДК и выработки рекомендаций и мер по противодействию деструктивам.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Формализация методического, алгоритмического и иных видов обеспечений для проектирования автоматизированной информационной системы (АИС ДК), обеспечивающей выявление в соцсети «ВКонтакте» генераторов ДК.

2. Формирование базы данных выявленных в соцсети «ВКонтакте» генераторов ДК, включая классификацию источников контента на основе метрик риск-анализа, распространяемых ими контентов.

3. Реализация возможности вывода результатов опытной эксплуатации, созданной АИС в удобном виде на примерах выявления генераторов ДК соцсети «ВКонтакте» за период спецоперации вооруженных сил Российской Федерации на Украине, включая выработку рекомендаций и мер по противодействию вышеуказанным деструктивам.

Планируемые результаты проекта:

1. Методическое и иное обеспечение необходимое для проектирования АИС обнаружения в соцсети «ВКонтакте» интернет-ресурсов, генерирующих контенты деструктивной направленности, а также собственно АИС ДК.

2. База данных выявленных в соцсети «ВКонтакте» источников-генераторов ДК, включая тематическую классификацию источников, а также – измерение их социальной опасности на основе риск-анализа распространяемых ими контентов.

3. Результаты опытной эксплуатации созданной АИС на примерах выявления источников-генераторов ДК соцсети «ВКонтакте» за период проведения специальной военной операции Вооруженных сил России на Украине, а также – рекомендации и меры по противодействию выявленным деструктивам.

Новизна результатов заключается в следующем:

1. Разработанные виды обеспечения АИС позволяют в отличии от аналогов в автоматизированном режиме выявлять генераторы противоправных контентов деструктивной направленности в соцсети ВКонтакте.

2. На основе разработанной методики АИС будет в отличии от аналогов может быть сформирована база данных генераторов противоправных контентов деструктивной направленности для соцсети «ВКонтакте», включающая их идентифицирующие данные, классификацию и уровень социальной опасности.

3. Выработанные на основе результатов опытной эксплуатации созданной АИС на примерах выявления генераторов противоправных контентов соцсети «ВКонтакте» (за период проведения специальной военной операции России на Украине) рекомендации и меры позволяют в отличии от аналогов обеспечить эффективное противодействие выявленным деструктивам.

Практическая ценность результатов видится в следующем:

1. Созданная АИС может быть практически использована компетентными органами России в борьбе с генераторами ДК за обеспечение региональной и национальной информационной безопасности.

2. Сформированная база данных генераторов ДК способна послужить основой для систематической работы с пользователями соцсети ВКонтакте по очищению этого социо-информационного пространства от деструктивных контентов.

3. Результаты опытной эксплуатации автоматизированной информационной системы по поиску и идентификации генераторов ДК могут послужить эффективной информационной базой для противоборства в пространстве социальных сетей, пользующихся популярностью у российских пользователей.

Теоретическая значимость заключаются в следующем:

1. Функциональные возможности предлагаемой автоматизированной информационной системы могут быть существенно расширены в результате соответствующих исследований вовлеченности пользователей в содержание ДК, включая их невиртуальные реакции.

2. Углубленный анализ генераторов и их контентов открывает перспективу модернизации базы данных с добавлением к ней аналитических блоков прогнозирования на основе машинного обучения.

3. Глубокая аналитика результатов опытной эксплуатации автоматизированной информационной системы позволит скорректировать ее алгоритмы и перенастроить программное обеспечение под растущие потребности информационного противоборства в социальных сетях, пользующихся популярностью у российской молодежи.

Вышеизложенное показывает, как практически может быть сформирована матрица (табл. 1) целеполагания и результативности в конкретной проектной деятельности по созданию АИС в интересах обеспечения информационной безопасности.

Схема использования АИС следующая:

1. На первом этапе проводится парсинг исследуемой социальной сети. Сканируя ее ресурсы (желательно с шагом не более одних суток), выявляем поступающие контенты, которые в дальнейшем подвергаются анализу по признакам деструктивности.

2. Далее с помощью соответствующих фильтров выявляются деструктивные контенты и идентифицируются с породившими их интернет-источниками.

3. Выявленные генераторы ДК классифицируются тематически и подвергаются риск-анализу.

4. Генераторы ДК вместе с их метриками помещаются в специализированную базу данных (БД), где они группируются по темам и ранжируются по степени опасности (рискам)

5. Цикл актуализации БД повторяется ежесуточно.

Блок-схема алгоритма, реализующего описанные выше процедуры, представлена на рис. 3.

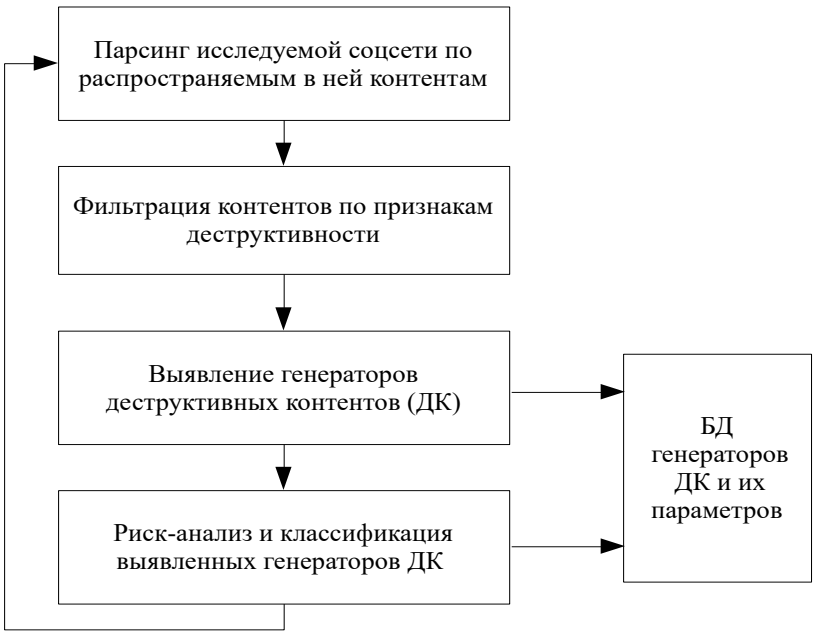

Рис. 3. Блок схема обобщенного алгоритма функционирования проектируемой АИС

Простейшую риск-оценку ДК можно сделать следующим образом:

$$\text{Risk} = \frac{[\text{количество генерируемых источником ДК в единицу времени}]}{[\text{общее количество контентов,созданных данным источником в единицу времени}]}. \quad (3)$$

Однако такая оценка (3) достаточно груба, так как контенты имеют различную степень вовлеченности пользователей. Поэтому уместно воспользоваться другой метрикой (4):

$$\text{Risk} = \frac{\left[\begin{array}{c}\text{количество пользователей,вовлеченных в содержание всех}\\ \text{сгенерированных источником ДК в единицу времени}\end{array}\right]}{[\text{общее количество контентов,созданных данным источником в единицу времени}]}. \quad (4)$$

При этом вовлеченность можно оценивать по количеству (в единицу времени) «лайков», «репостов» и «позитивных комментариев» по ДК. Это легко сделать по каждой из вышеуказанных реакций в отдельности, а также интегрально через их сумму:

$$k_V = k_{(\text{лайк})} + k_{(\text{репост})} + k_{(\text{коммент})} \quad (5)$$

Уместно учесть в (5) пересечения, когда один и тот же пользователь выдает одновременно несколько указанных позитивных реакций на ДК. Это позволит повысить точность оценки опасности источника ДК.

Что же касается интервала времени, в течение которого ведется измерение, то зачастую для этого используется среднее время жизни контента в сети (обычно не более суток).

Алгоритмически вышеизложенное можно формализовать с помощью рис. 4.

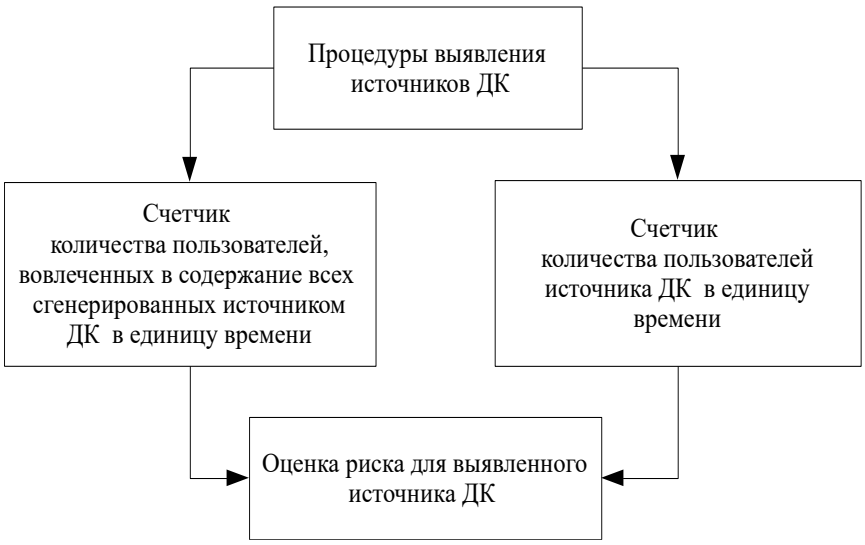

Рис. 4. Блок-схема алгоритма модуля риск-оценки источника ДК

Формат данных БД генераторов ДК обобщенно можно представить следующим образом:

ID источника ДК	Тематическая направленность источника	Risk

Таким образом в БД можно выбрать источники ДК со схожей тематической направленностью, а также проранжировать их по уровню социальной опасности (риску). Такую последовательность действий следует реализовать для генераторов ДК в отношении специальной военной операции ВС РФ на Украине.

Заключение

Предложенная матричная формализация (табл.1) применима и для проектирования других систем и задач, например, в случае проектной деятельности в отношении масштабных исследований угроз информационному пространству Российской Федерации (ИПРФ). Так, столбец задач матрицы формализации может в этих исследованиях выглядеть следующим образом:

1. Анализ арсенала средств и их классификация для деструктивных воздействий противника на заданную сферу ИПРФ.

2. Систематизация и исследование данных (статистических и иных), характеризующих ущербы, наносимые противником в заданной сфере ИПРФ посредством атак с помощью вышеуказанного арсенала.

3. С помощью общепринятых критериев (для рассматриваемой сферы) оценка (желательно в динамике противоборства) возникающих рисков достижения пороговых значений устойчивости ИПРФ.

4. На основе полученных результатов исследования выработка конкретных (правовых, организационных и др.) мер по укреплению (снижению вышеуказанных рисков) защищенности заданной сферы ИПРФ.

Алгоритм перечисленных действий иллюстрирует рис. 5.

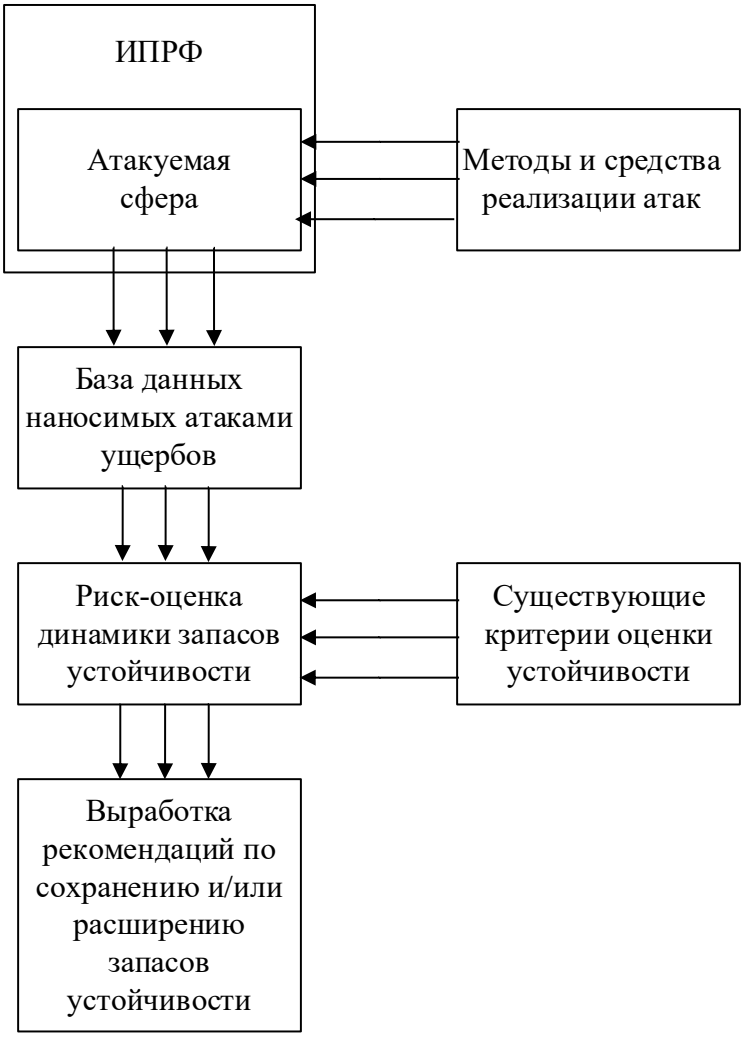

Рис. 5. Структурная схема риск-анализа атакуемой сферы ИПРФ

Аналитически риск-оценку можно осуществить следующим образом:

$$\mathrm{Risk} = \frac{К_{АДП}}{k_{кр} К_{НС}}, \qquad (6)$$

где $К_{АДП}$ – количество адептов деструктивного (по отношению к исследуемому социуму) проекта;

$k_{кр}$ - критический (с точки зрения устойчивости социума) уровень адептов деструктивного проекта (обычно измеряется в %);

$К_{НС}$ – численность населения исследуемого социума;

$\overline{К_{НС}}=k_{кр}К_{НС}$ – пороговое значение нарушения устойчивости социума.

В этой формуле Risk = 0÷1, а запас устойчивости можно относительно оценить как:

$$Z = 1 - \mathrm{Risk}. \qquad (7)$$

При этом, критерии устойчивости частично известны [2, 6] и из них следует настраивать параметр (7) под размерность формулы (6). В свою очередь параметр $К_{АДП}(t)$ следует искать (в динамике времени t) в соответствующих соцопросах. Тогда станет ясна и динамика рисков.

Приведенный пример свидетельствует о широте спектра применения матричной формализации: от специализированных АИС обеспечения кибербезопасности [1, 3-5, 7] до глобальных информационных проблем (мультигендерность, русофобия, искажение истории и т. п.), разрешение которых приобретает особую остроту на современном разломе однополярного мироустройства.

Поэтому предлагаемое в настоящей работе методическое обеспечение с успехом может быть использовано студентами соответствующих специальностей при подготовке отчетов по практике,

пояснительных записок к курсовым проектам и выпускных квалификационных работ. Особенно полезна матрица формализации для аспирантов, докторов и научных работников, занимающихся проектной деятельностью в сфере защиты информации и обеспечения информационной безопасности [7].

Список литературы

1. Остапенко А.Г. Эпидемии в телекоммуникационных сетях / А.Г. Остапенко, Н.М. Радько, А.О. Калашников [и др.]; Под ред. чл.-корр. РАН Д.А. Новикова // М.: Горячая линия – Телеком, 2018. 282 с.

2. Остапенко А.Г. Атакуемые взвешенные сети / А.Г. Остапенко, Д.Г. Плотников, А.О. Калашников [и др.]; Под ред. чл.-корр. РАН Д.А. Новикова // М.: Горячая линия – Телеком, 2018. 246 с.

3. Остапенко А.Г. Социальные сети и деструктивный контент / А.Г. Остапенко, А.В. Паринов., А.О. Калашников [и др.]; Под ред.чл.-корр. РАН Д.А. Новикова // М.: Горячая линия – Телеком, 2018. 276 с.

4. Остапенко А.Г. Социальные сети и риск-мониторинг / А.Г. Остапенко, Е.Ю. Чапурин, А.О. Калашников [и др.]; Под ред.чл.-корр. РАН Д.А. Новикова // М.: Горячая линия – Телеком, 2019. 266 с.

5. Остапенко А.Г. Социальные сети и психологическая безопасность / А.Г. Остапенко, Е.Б. Белов, А.О. Калашников [и др.]; Под ред.чл.-корр. РАН Д.А. Новикова // М.: Горячая линия – Телеком, 2021. 232 с.

6. Остапенко А.Г. Сетео-информационная эпидемиология / А.Г. Остапенко, Е.Б. Белов, А.О. Калашников [и др.]; Под ред.чл.-корр. РАН Д.А. Новикова // М.: Горячая линия – Телеком, 2021. 216 с.

7. Остапенко А.Г. Картография защищаемого киберпространства / А.Г. Остапенко, А.Л. Сердечный, А.О. Калашников; Под ред.чл.-корр. РАН Д.А. Новикова // М.: Горячая линия – Телеком, 2022. 372 с.

Финансовый университет при Правительстве Российской Федерации
Financial University under the Government of the Russian Federation

Воронежский государственный технический университет
Voronezh State Technical University

Поступила в редакцию 01.09.22

Информация об авторах

Остапенко Григорий Александрович – д-р техн. наук, проректор Финансового университета при Правительстве Российской Федерации, e-mail: mnac@comch.ru

Белоножкин Владимир Иванович – д-р техн. наук, профессор Воронежского государственного технического университета, e-mail: mnac@comch.ru

Баранников Николай Ильич – д-р техн. наук, профессор Воронежского государственного технического университета, e-mail: mnac@comch.ru

Остапенко Александр Алексеевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Краснобородкин Александр Геннадьевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Мирошниченко Татьяна Юрьевна – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

MATRIX FORMALIZATION OF GOAL-SETTING AND PERFORMANCE OF PROJECT ACTIVITIES IN THE FIELD OF INFORMATION PROTECTION AND INFORMATION SECURITY

G.A. Ostapenko, V.I. Belonozhkin, N.I. Barannikov, A.A. Ostapenko, A.G. Krasnoborodkin, T.Yu. Miroshnichenko

The work is devoted to the actual problem of formalizing the goals, objectives and expected results of project activities when creating information-protected systems. In this regard, it is proposed to build a matrix of goal-setting and project effectiveness, in which the columns refer to the contradictions identified at the preliminary stage, the tasks of resolving these contradictions, the expected results of solving the tasks, their characteristics of novelty, practical and theoretical significance. In turn, each row of the matrix is focused on a specific design problem. In general, goal setting is based on the planned characteristics of the chance of usefulness and the risk of inferiority of the system being created, for which analytical security metrics are proposed and the field of project activity is formalized. Examples are given of constructing the necessary formalisms for information security systems, as well as methods for calculating risks.

Keywords: matrix, formalization, goal setting, performance, project activities, information protection, information security.

Submitted 1.09.22

Information about the authors

Grigory A. Ostapenko – Dr. Sc. (Technical), Vice-Rector of the Financial University under the Government of the Russian Federation, e-mail: mnac@comch.ru

Vladimir I. Belonozhkin - Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

Nikolai I. Barannikov - Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

Alexander A. Ostapenko – student, Voronezh State Technical University, e-mail: mnac@comch.ru

Alexander G. Krasnoborodkin – student, Voronezh State Technical University, e-mail: mnac@comch.ru

Tatyana Yu. Miroshnichenko – student, Voronezh State Technical University, mnac@comch.ru