**DOI 10.36622/VSTU.2023.26.2.002**
**УДК 004.056**

# МЕТОДИЧЕСКИЕ ОСНОВЫ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ПРИ ВЫПОЛНЕНИИ НАУЧНО-ИССЛЕДОВАТЕЛЬСКОЙ РАБОТЫ СТУДЕНТАМИ СПЕЦИАЛИТЕТА В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**А.Г. Остапенко, А.С. Пахомова, Д.А. Нархов, А.А. Остапенко, А.И. Шеншин**

В статье рассматриваются научно-методические основы реализации научно-исследовательской работы студентами специальностей в сфере обеспечения информационной безопасности. В этой связи предлагаются шаблоны формулировки противоречий и актуальности проводимого исследования. Представлены научно-обоснованные методики целеполагания, включая постановку объекта и предмета исследования, цели и задач исследования в области обеспечения информационной безопасности. К тому же предлагаются рекомендации по решению постановленных задач в условиях современного информационного противоборства государств и транснациональных корпораций. Научно-методические рекомендации, предлагаемые в статье, обильно проиллюстрированы в виде соответствующих таблиц и рисунков, позволяющих исследователю наглядно по аналогии с упомянутым иллюстративным материалом осуществлять целеполагания для своей тематики. Рассматриваются также перспективы совершенствования результатов настоящей работы в части выявления угроз, проведения риск-анализа и управления информационными рисками в ходе реализации научно-исследовательской работы студентов.

Ключевые слова: исследование, риск, безопасность, цель, задачи, объект и предмет исследования.

Научно-исследовательская работа студентов (НИРС) в рамках учебного плана специальностей в сфере информационной безопасности имеет особое значение. В завершении четвертого курса, когда первичные профессиональные навыки студентом уже приобретены, представляется возможным провести репетицию подходов для дипломного проектирования, определиться с его содержанием и ожидаемым результатом. Поэтому важнейшим элементом НИРС является целеполагание, обеспечивающее формулировку цели и задач, для избранных объекта и предмета исследования. Системный подход для реализации этого обуславливает глубину и практическую и теоретическую результативность НИРС, что будет весьма полезно для последующего дипломного проектирования.

В профессиональной сфере обеспечения информационной безопасности целью исследования, как правило, выступает повышение защищенности атакуемой системы за счет оценки и регулирования, возникающих в данном случае рисков [1-7]. Перечисленные монографии, касающиеся вирусных воздействий [1,6], социо-информационной экспансии [3-5] или противоборства в киберпространстве [2,7], в целеполагании проектной деятельности ищут ответы на вопросы:

- в чем состоит сущность возникающих угроз,
- как через риски оценить степень опасности этих угроз,
- как повысить защищённость от рассматриваемых угроз путем регулирования измеренных рисков, в этом числе в условиях формирования многополярного мира.

В настоящей статье предполагается раскрывать научно-методические основы поиска ответ на вышеперечисленные вопросы в профессиональной области человеческих знаний, посвященной обеспечению информационной безопасности личности, общества и государства.

Спектр тематики НИРС достаточно широк, и поэтому предлагаемые в работе методики и рекомендации будут носить довольно обобщенный характер. Авторами исследований далее нужно адаптировать предлагаемые шаблоны к заданной им

© Остапенко А.Г., Пахомова А.С., Нархов Д.А., Остапенко А.А., Шеншин А.И., 2023

тематике и специфике подлежащих рассмотрению объектов.

Актуальность и практическую направленность исследования существенно усилит его реализация в контексте современных трендов формирования справедливого многополярного мира. Очевидно, что эта неотвратимая тенденция накладывает значительный отпечаток на угрозы развития планетарного и отечественного информационного пространства, что и должно найти свое отражение в результатах исследования, особенно в условиях той гибридной войны, которую развязал Коллективный Запад в отношении Российской Федерации. Думается, свой отпечаток на процесс реализации НИРС должна оставить и Специальная военная операция Вооруженных сил России на Украине.

Методологию вышеупомянутого исследования удобнее было бы раскрыть на примерах постановки исследовательских задач для наиболее перспективных тематик НИРС. Наглядность проектной деятельности, которая будет проиллюстрирована таблицами, позволит студенту по аналогии успешной сформулировать собственные цель и задачи. Прием аналогии во многом сокращает время выполнения проектных операций и позволяет наиболее полно учесть опыт предшествующих исследований по заданной тематике.

Задание по выполнению НИРС традиционно указывает на объект, подлежащий исследованию. В свою очередь предмет исследования (в профессиональной нашей среде) сводится к оценке и регулированию рисков, относящихся к объекту исследования. Здесь проектанту не потребуется проявить особую самостоятельность, ведь состояние безопасности достигается, когда риск реализации угроз не превышает допустимых значений. Проблемой, конечно, будет измерение значений риска. Здесь придется идентифицировать негативы, связанные с объектом, оценить масштабы их проявления в виде соответствующих ущербов, а также провести риск-анализ.

Объект исследования, как правило, рассматривает пространство, подвергающееся атакам злоумышленника. Это может быть непосредственно общество и/или технические системы, обеспечивающие его функционирование. В первом случае речь идет о деструктивном информационно-психологическом воздействии на личность и группы людей, а во втором – о кибератаках.

Если отслеживать патриотическую тематику, то нас, в первую очередь, должно интересовать отечественное информационное пространство: социо-информационная и кибер-информационная его составляющие, подвергающиеся атакам противника, который также должен быть поименован в объекте исследования. Это множество, в условиях перехода к многополярному миру, практически неисчерпаемо. Здесь можно встретить прозападные кибервойска, подконтрольные Западу интернет-гиганты, деструктивные продукты игровой индустрии и т.п. Соответствующие формулировки предмета исследования можно увидеть в примерах, приведенных в табл. 1-3.

Относительно предмета исследования уместно заметить следующее. В наших специальностях, прежде всего, интересует обеспечение безопасности, которое напрямую связано с оценкой и регулированием создаваемых противником рисков. Отражение этого факта также встречается в табл. 1-3, как и во всех других тематический исследованиях специальностей в сфере защиты информации и обеспечения информационной безопасности.

На основании вышеизложенного представляется возможным сформулировать цель исследования. Она, очевидно, должна состоять в том, чтобы повысить защищенность объекта за счет оценки и регулирования выявленных рисков, создаваемых противником. Механизм формулировки иллюстрирует рис. 1, а примеры применения этого механизма представлены в табл. 1-3. Разумеется, что целеполагание должно быть конкретизировано под тему исследования в используемых терминах и формулировках.


Рис. 1. Иллюстрация механизма целеполагания исследования

Таблица 1

Пример целеполагания для исследования деструктивной деятельности прозападных кибервойск

| **Объект исследования** |
|---|
| Кибервойска Коллективного Запада, атакующие информационное пространство России |
| **Предмет исследования** |
| Риски нарушения безопасности отечественного информационного пространства в результате деструктивной деятельности прозападных кибервойск |
| **Цель исследования** |
| Повышение защищенности отечественного информационного пространства и общества за счет оценки и регулирования рисков деструктивной деятельности кибервойск Коллективного Запада |
| **Задачи исследования** |
| 1. Исследование методов и средств деструктивной деятельности прозападных кибервойск, включая выявление создаваемых ими угроз для российского общество и государства.<br>2. Сбор статистики результатов деструктивной деятельности прозападных кибервойск, включая оценку рисков нарушения ими информационной безопасности России.<br>3. Выработка методик и алгоритмов технического и организационно-правового регулирования рисков нарушения общественной информационной безопасности, создаваемых деструктивной деятельностью кибервойск. |

Таблица 2

Пример целеполагания для исследования деструктивного воздействия игровой индустрии

| **Объект исследования** |
|---|
| Российское общество и государство в условиях деструктивного воздействия продуктов игровой индустрии |
| **Предмет исследования** |
| Риски нарушения безопасности отечественного общества и государства, создаваемые распространением деструктивных продуктов игровой индустрии |
| **Цель исследования** |
| Повышение защищенности отечественного общества и государства за счет оценки и регулирования рисков нарушения социо-информационной безопасности граждан России, создаваемых распространением деструктивных продуктов игровой индустрии |
| **Задачи исследования** |
| 1. Исследование деструктивного влияния продуктов игровой индустрии и выявление угроз нарушения безопасности российского общества и государства, создаваемых ими.<br>2. Сбор статистики результатов распространения деструктивных продуктов игровой индустрии, включая аналитическую оценку создаваемых ими рисков.<br>3. Выработка методик и алгоритмов регулирования рисков нарушения социо-информационной безопасности России, создаваемых внедрением деструктивных информационных продуктов игровой индустрии. |

Таблица 3

Пример целеполагания для исследования деструктивного влияния интернет-гигантов

| **Объект исследования** |
|---|
| Отечественное общество и государство, подвергающиеся деструктивному информационному воздействию со стороны интернет-гигантов |
| **Предмет исследования** |
| Риски нарушения информационной безопасности России, создаваемые деструктивной деятельностью интернет-гигантов |
| **Цель исследования** |
| Повышение защищенности российского общества и государства за счет оценки и регулирования рисков нарушения безопасности отечественного информационного пространства в результате деструктивной деятельности интернет-гигантов |
| **Задачи исследования** |
| 1. Исследование деструктивного влияния интернет-гигантов и выявление угроз нарушения информационной безопасности России в результате этого влияния.<br>2. Сбор статистики результатов деструктивной деятельности интернет-гигантов, включая аналитическую оценку создаваемых ими рисков.<br>3. Выработка методик и алгоритмов регулирования рисков нарушения информационной безопасности России, создаваемых для российского общества интернет-гигантами. |

Четкая формулировка цели исследования открывает перспективу к адекватной постановке его задач. На рис. 1 предлагается методический подход для этого. В этой связи в соответствии с выявленными противоречиями рассматриваются три основных типа задач.

1. Объективно необходимо исследование методов и средств, используемых противником для деструктивного воздействия на объект. Здесь принципиально установить перечень и опасность угроз, создаваемых в данном случае злоумышленниками.

2. Установленные угрозы должны быть исследованы в части статистики частоты и ущербности их реализации. Эти данные послужат основой для аналитической риск-оценки объекта в условиях деструктивного воздействия на него противника.

3. Венцом исследования, очевидно, должны быть методики, алгоритмы и их практическое применение в части регулирования рассматриваемых рисков. Здесь объективно необходимы оценки эффективности предлагаемого инструментария риск-управления на объекте.

Иллюстрацией для применения вышеизложенного механизма служит рис. 1.

Научно-методические рекомендации по решению поставленных задач исследования могут быть сведены к следующему.

1. Необходимы детальное и системное рассмотрение арсеналов противника в контексте их применения на объекте. Здесь уместен анализ методов и средств, применяемых противником с целью дестабилизации отечественного информационного пространства и нарушения национальной безопасности. В этом случае весьма важна полнота рассмотрения всего множества видов информационного оружия, наносящего нам ущерб. Только в этом случае мы будем в состоянии выявить все многообразие явных и скрытых угроз, оценить степень их опасности для российского общества и государства. Это важно сделать по каждому деструктиву, который несет нам противник, имея ввиду частоту и ущербность его применения. Фактически на данном этапе исследования определяется номенклатура угроз и инструментов их реализации противником в отношении защищаемого объекта. Полученные при этом данные послужат основой для следующего этапа работы, обеспечивающего риск-анализ деструктивов, порожденных применением рассматриваемого многообразия типов информационного оружия [4,5,7].

2. Риск-анализ является неотъемлемой частью исследования, ибо безопасность есть состояние объекта, при котором риск реализации угроз не превышает допустимых значений. Оценку риска по каждому деструктиву, выявленному на предшествующем этапе исследования, возможна на основе формирования статистики, показывающей величину наносимого ущерба и частоту его появления при использовании противниками рассматриваемого информационного оружия. Многочисленные интернет-источники предоставляют пользователям широкий спектр подобной информации, которая при соответствующей её обработке может лечь в основу необходимого риск-анализа. При этом надо понимать, что риск, обычно измеряемый произведением величины ущерба на вероятность его появления, по большому счету представляет собой функцию зависимости от дискретизированного ущерба. Поэтому желательно располагать такими данными по всему многообразию информационного оружия, определяемого темой исследования. Результаты риск-анализа послужат основой для следующего этапа работы, где предполагается повысить защищенность рисков, порождаемых применением рассматриваемого типа информационного оружия [2,3,6].

3. Важнейшим результатом исследования являются методики и алгоритмы регулирования аналитически определенных рисков. Снижение этих рисков в заданном диапазоне ущербов следует считать необходимым условием повышения защищенности объекта исследования. При этом необходимо понимать, что минимизация рисков на всем множестве значений ущерба принципиально невозможна из-за вероятностной его природы. Однако поиск программно-технических и/или организационно-правовых решений вышеуказанной задачи не является безнадежным, прежде всего в зонах повышенной ущербности объекта исследования. На них обязательно укажут результаты ранее проведенного риск-анализа, если конечно он проводился адекватно и детально. При этом выбор и даже генерация средств регулирования должны осуществляться в прямой зависимости и с учетом специфики несущих противником деструктивов. Особую значимость имеет оценка эффективности предлагаемого инструментария регулирования рисков, осуществляемая по принципу сравнения значений риска до и после его применения. Это можно сделать экспериментально либо аналитически. Именно тогда работа будет иметь относительно законченный характер и её результаты могут служить объективной основой для последующих исследований по настоящей теме.

Наряду с численным сравнением, рассмотренным выше, необходимо еще и качественная оценка достоинств полученных в исследовании результатов. Сравнение традиционно следует осуществлять с аналогами, которые могут быть почерпнуты, в том числе, из информационных источников, поименованных в монографиях [1-7]. Такой качественный анализ необходим

для адекватного осознания особенности полученных в исследовании результатов и определения путей их дальнейшего совершенствования.

Этот подход эффективно используется для оценки новизны продуктов исследования. Здесь применяются, почерпнутые из патентоведения две формулы «впервые» и «в отличии от аналогов». Впервые получаются, как правило, пионерские результаты. Например, когда отсутствуют прямые аналоги, либо в том случае, когда к описанию известного также известный аппарат, скажем риск-анализ.

Вторую формулировку удобнее проиллюстрировать на примере решения первой обобщенной задачи, сформулированной для исследования в настоящей работе. Здесь, в отличии от аналогов, обычно проявляется новизна в более полном рассмотрении множества угроз, уязвимостей и сценариев атак. Формулировка «впервые» в данном случае зачастую звучит при организации комплексного рассмотрения вышеупомянутых множеств, скажем при построении риск-ландшафта. В отношении второй обобщенной задачи исследования, обозначенной в настоящей работе, новизна может проявляться в специфике анализируемого объекта, которая потребует специальной аналитики оценки ущербов и вероятности их наступления. К примеру, это может быть доля адептов в общем множестве авторов исследуемого пространства.

Наконец, в решении третьей обобщенной задачи обычно почти все аналитические выкладки относительно методик и алгоритмов управления, если, конечно, они корректны, обладают необходимой новизной, ибо регулировка рисков по-прежнему остается фигурой высшего пилотажа в теории и практике обеспечения информационной безопасности. Здесь вполне допустима формула «впервые», если исследователь не ограничился банальным словоблудием, а получил вполне конкретные результаты повышения защищенности объекта.

Практическая ценность исследования во многом определяется её актуальностью и выявленными в нем противоречиями. В отличии от оценки новизны, где исследователь стремится отмеживаться от аналогов, при формулировке признаков практической ценности результатов ему необходимо определиться с квазианалогами, где возможна конкретная реализация полученного продукта. Фактически нужно указать где и как ожидается внедрение результатов исследования с учетом специфики текущего момента. Чем эффективней продукт, тем шире пространство его применения в современных условиях мирового переустройства.

В структурном плане приведенные в настоящей работе элементы (для постановки исследования) рекомендуется сконцентрировать во введении пояснительной записки в следующей последовательности:

- актуальность исследования;
- аналоги и противоречия;
- объект исследования;
- предмет исследования;
- цель;
- задачи исследования;
- результаты, выносимые на защиту;
- новизна результатов:
- практическая ценность.

Такая компановка позволит самому исследователю и его оппонентам быстрее и четче понять суть работы, а также – формализовать презентационный материал к защите.

Научно-методические знания и навыки, полученные исследователем при выполнении НИРС, послужат весьма полезной основой как в подготовке выпускной (научной) квалификационной работы студента (аспиранта), так и во всех последующих творческих проектах, реализуемых специалистом для обеспечения информационной безопасности личности, общества и государства в суровых условиях формирования справедливого многополярного мироустройства.

Представленный в настоящей статье научно-методический подход проведения НИРС может быть с успехом использован при осуществлении дипломного и курсового

проектирования по специальностям в сфере обеспечения информационной безопасности. Он также будет полезен аспирантам в ходе написания ими научно-квалификационной работы.

Развитие результатов предложенной методологии видится на пути конкретизации приемов реализации оценки рисков с учетом специфики объекта исследования и многообразия возникающих для него угроз, имея ввиду динамику развития информационного противоборства в условиях формирования справедливого многополярного мира.

Особый научный и практический интерес представляет совершенствование методик и алгоритмов управления выявленными и измеренными рисками нарушения информационно безопасности. Здесь важным аспектом выступает выбор диапазонов ущербов подлежащих регулированию вероятности их наступления, а также - средств, способных обеспечить эффективное управление процессом повышения защищенности объекта исследования.

В целом статью можно рассматривать как преддверие построения теории синтеза систем с заданными риск-характеристиками в условиях нарастающего информационного противоборства государств и транснациональных гигантов.

Обозначенные направления совершенствования проектной деятельности будут особенно полезны выпускникам специалитета, планирующим связать свою профессиональную карьеру с научным поиском в сфере обеспечения информационной безопасности личности, общества и государства.

**Список литературы**

1. Эпидемии в телекоммуникационных сетях / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 1).

2. Атакуемые взвешенные сети / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 2).

3. Социальные сети и деструктивный контент / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2017. – 284 с. (Серия «Теория сетевых войн»; вып. 3).

4. Социальные сети и риск-мониторинг / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2019. – 284 с. (Серия «Теория сетевых войн»; вып. 4).

5. Социальные сети и психологическая безопасность / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2020. – 284 с. (Серия «Теория сетевых войн»; вып. 5).

6. Сетео-информационная эпидемиология / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2021. – 284 с. (Серия «Теория сетевых войн»; вып. 6).

7. Картография защищаемого киберпространства / Остапенко [и др.]; [под ред. чл. – корр. РАН Д.А. Новикова]. – М: Горячая линия – Телеком, 2022. – 372 с. (Серия «Теория сетевых войн»; вып. 7).

ФГБОУ ВО «Воронежский государственный технический университет»
Voronezh State Technical University

Поступила в редакцию 10.04.2023

**Информация об авторах**

**Остапенко Александр Григорьевич –** д-р техн. наук, заведующий кафедрой, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Пахомова Анна Степановна** – канд. техн. наук, доцент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Нархов Дмитрий Андреевич** – студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

**Остапенко Александр Алексеевич –** студент, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com
**Шеншин Александр Игоревич** – аспирант, Воронежский государственный технический университет, e-mail: alexanderostapenkoias@gmail.com

# METHODOLOGICAL FOUNDATIONS OF PROJECT ACTIVITY WHEN PERFORMING RESEARCH WORK BY STUDENTS OF THE SPECIALTY IN THE FIELD OF INFORMATION SECURITY

**A.G. Ostapenko, A.S. Pakhomova, D.A. Narkhov, A.A. Ostapenko, A.I. Shenshin**

The article discusses the scientific and methodological foundations of the implementation of research work by students of specialties in the field of information security. In this regard, templates for the formulation of contradictions and the relevance of the study are proposed. The article presents scientifically-based methods of goal-setting, including the formulation of the object and subject of research, goals and objectives of research in the field of information security. In addition, recommendations are proposed for solving the tasks set in the conditions of modern information warfare between states and transnational corporations. The scientific and methodological recommendations proposed in the article are abundantly illustrated in the form of appropriate tables and figures, allowing the researcher to visually, by analogy with the above-mentioned illustrative material, carry out goal-setting for his subject. The prospects of improving the results of this work in terms of identifying threats, conducting risk analysis and managing information risks during the implementation of students' research work are also considered.

Keywords: research, risk, safety, purpose, objectives, object and subject of research

Submitted 10.04.2023

**Information about the authors**
**Alexander G. Ostapenko –** Dr. Sc. (Technical), Head of the Department, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
**Anna S. Pakhomova** – Cand. Sc. (Technical), Associate Professor, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
**Dmitry A. Narhov** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
**Alexander A. Ostapenko** – student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com
**Alexander I. Shenshin** – postgraduate student, Voronezh State Technical University, e-mail: alexanderostapenkoias@gmail.com