DOI 10.36622/VSTU.2022.25.2.004
УДК 001.89 : 004.77

СПЕЦИАЛИТЕТ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»: КРАТКИЕ НАУЧНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ПОДГОТОВКИ ВЫПУСКНЫХ КВАЛИФИКАЦИОННЫХ РАБОТ

К.А. Разинкин, В.Н. Кострова, В.М. Питолин, Е.С. Соколова, Д.А. Нархов, А.Е. Прохорова

В статье описаны основные научно-методические рекомендации для подготовки выпускных квалификационных работ. Озвучена основная терминология, которая применяется в ходе дипломного проектирования и особенности классифицированного дерева, способствующего фундаментальному анализу угроз и рисков. Перечислены (в контексте исследования) пункты, основной мыслью которых является недопустимость использования информации, не имеющей под собой достаточно мощную теоретическую и доказательную базу. Прописаны рекомендации по подготовке выпускной квалификационной работы. Работа ориентирована на специальности «Информационная безопасность телекоммуникационных систем», «Информационная безопасность автоматизированных систем» и «Компьютерная безопасность». Предложения, сформулированные в ней, учитывают опыт подготовки и защиты ВКР по вышеуказанным специальностям, сложившийся в Воронежском государственном техническом университете. Стремительное нарастание множества и опасности информационных рисков, порождаемых революционной цифровой трансформацией личности, общества и государства, обуславливает практическую актуальность научно-методических рекомендаций настоящей работы для дипломников, их руководителей и выпускников кафедр специалитета «Информационная безопасность».

Ключевые слова: риск, угрозы, выпускная квалификационная работа, аналитическая оценка, объект и предмет исследования, противоречия, результаты.

Введение

В настоящее время особую значимость приобретает привитие будущим специалистам навыков структурирования и формализации исследовательской деятельности в форматах, принятых научно-техническим обществом. Особую актуальность вышеизложенная задача имеет для специальностей в сфере информационной безопасности (ИБ), где обновление контента и технологий происходит с гигантской скоростью, а выпускник, лишенный аналитических навыков, не сможет эффективно создавать и защищать вверенные ему информационные ресурсы [1-6]. В этой связи, в структуре подготовки выпускника специалитета по УГСН 10.00.00 «Информационная безопасность» особую актуальность приобретает интегральная оценка уровня сформированности компетенций выпускника и его готовности к профессиональной деятельности в рамках государственной итоговой аттестации в виде выпускной квалификационной работы.

В соответствии с Федеральным Законом Российской Федерации №273-ФЗ от 29 декабря 2012 года «Об образовании в Российской Федерации» и соответствующими Приказами Минобрнауки России утверждающими Федеральные государственные образовательные стандарты высшего образования по специальностям 10.05.01 «Компьютерная безопасность» (№1459 от 26 ноября 2020 г.) , 10.05.02 «Информационная безопасность телекоммуникационных систем» (№ 1458 от 26 ноября 2020 г.) и 10.05.03 «Информационная безопасность автоматизированных систем» (№ 1457 от 26 ноября 2020 г.) (уровень специалитета)», итоговая государственная аттестация студентов, завершающих обучение по программам высшего образования в высших учебных заведениях, в том числе и по

программе специалитета по указанным направлениям, является обязательной.

Итоговая государственная аттестация включает защиту выпускной квалификационной работы (ВКР). ВКР, являясь заключительным этапом обучения студентов, имеет своей целью:

- систематизацию, закрепление и расширение теоретических знаний и практических навыков проектирования системы защиты информационных процессов,
- технологий, систем и сетей, а также их инструментального (программного, технического, организационного) обеспечения;
- развитие навыков самостоятельной работы, четкого и логичного формулирования своих мыслей, публичной защиты предлагаемых решений.

Вместе с тем, с учётом компетентностного подхода к подготовке специалистов для реализации части основной образовательной программы, формируемой участниками образовательных отношений, были выбраны следующие профессиональные стандарты:

- 06.030 «Специалист по защите информации в телекоммуникационных системах и сетях», утвержденный приказом Министерства труда и социальной защиты Российской Федерации 03 ноября 2016 г. № 608н;
- 06.032 «Специалист по безопасности компьютерных систем и сетей», утвержденный приказом Министерства труда и социальной защиты Российской Федерации 01 ноября 2016 г. №598н;
- 06.033 «Специалист по защите информации в автоматизированных системах», утвержденный приказом Министерства труда и социальной защиты Российской Федерации 15 сентября 2016 г. № 522н;

Исходя из требований ФГОС и трудовых функций, изложенных в профессиональных стандартах и рекомендациях учебно-методического объединения высших учебных заведений России по образованию в области информационной безопасности, а также научного направления выпускающей кафедры, одной из ведущих проблем в области обеспечения информационно безопасности является противоборство в ходе реализации сетевых информационных операций и атак. Она обусловлена избыточностью в эмпирических материалах, казуальных схемах, концептуальных и доктринальных нормах декларативной бланкетной направленности и дедуктивными недостатками в материальном и виртуальном мире, инфраструктуре, общих моделях, универсальном регулировании [1-3].

Таким образом, становится очевидной необходимость формирования комплексных интегративных подходов к рассмотрению информационных операций и атак как стадий информационных конфликтов и противоборств социотехнических систем [4-6].

Теоретические положения

В этом контексте ИБ-выпускнику необходимо продемонстрировать компетенции в области обеспечения безопасности – состояния защищенности исследуемого объекта (вида, класса объектов) от заданного множества угроз (атак, уязвимостей), при котором значения (в определенных диапазонах ущербов) риска не превышают допустимого уровня. На рис. 1 представлен примерный алгоритм менеджмента риска информационной безопасности, рекомендуемый к реализации студентам в рамках выпускных квалификационных работ [7-9].

Таким образом, предметом исследования выступает оценка и регулирование риска реализации угроз (совокупности факторов, способных привести к ущербу в объекте). Измерение риска (вероятной возможности наступления ущерба определенной величины) осуществляется на основе статистических и/или экспериментальных данных, которыми располагает дипломник в отношении объекта исследования. При этом автор должен убедительно продемонстрировать эффективность предложенных им технических решений и/или методов для достижения цели ВКР (повышения защищенности объекта).

Фундаментально определяющим базу исследования является дерево угроз и рисков, которое устанавливает причинно-следственную взаимосвязь выявленных угроз и индуцированных ими рисков. Это квалификационное дерево имеет в качестве корневой основы системно-образующие угрозы, от которых разветвляются цепочки рисков. Исследование должно неукоснительно следовать данному дереву, которое, в свою очередь, обязано обеспечивать полноту рассмотрения и учета всего множества угроз и рисков (фрагментарный анализ не допустим).

Когда множество угроз и вытекающих из них рисков определено, то можно приступать к риск-анализу. Высшим пилотажем здесь является их оценка с помощью полученных аналитических выражений. Однако чаще всего приходится опираться на данные статистики (причем не только отечественной, но и зарубежной).

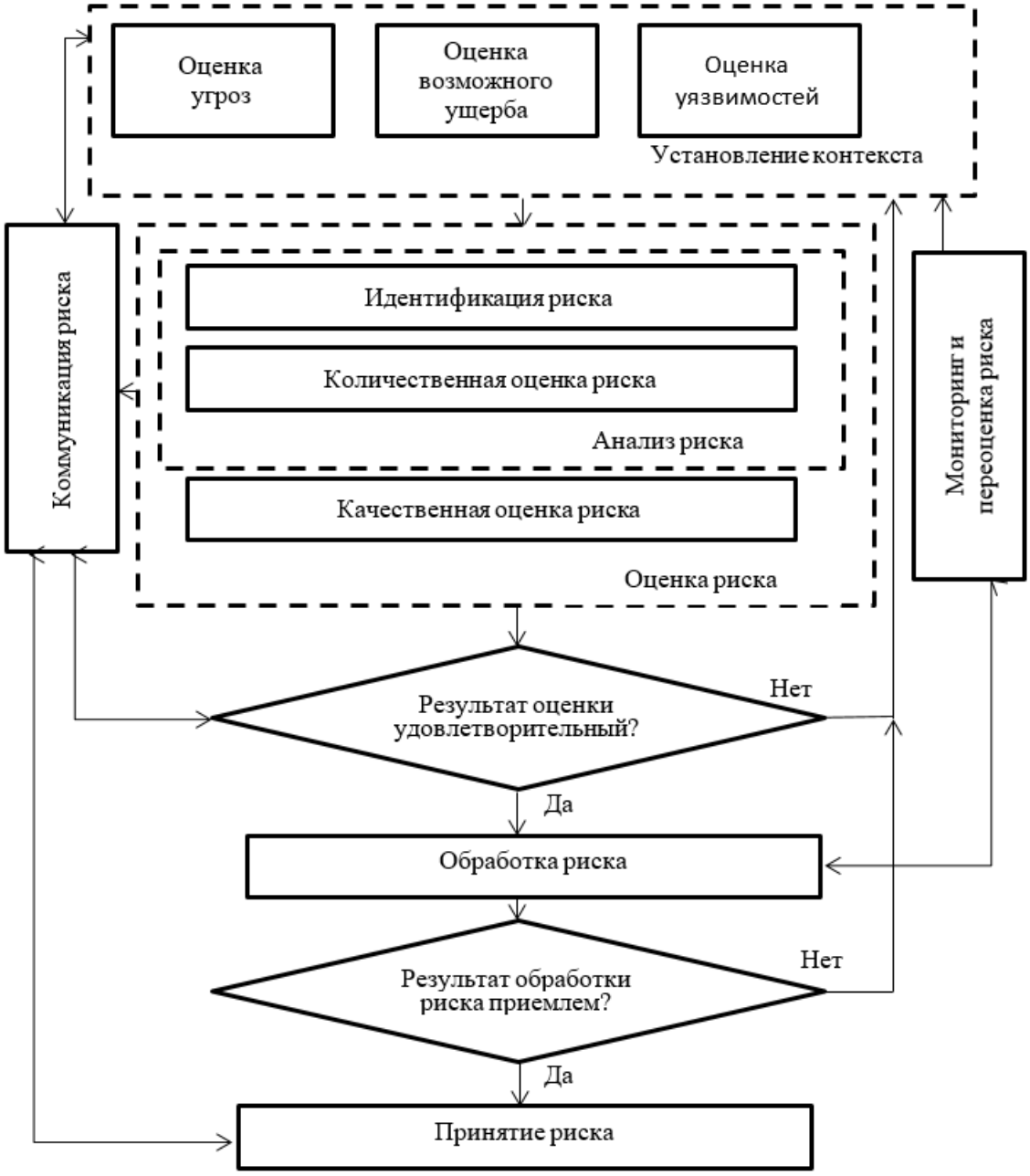

Рис. 1. Процесс менеджмента риска информационной безопасности

Для социотехнических угроз зачастую используют данные социологических опросов населения у нас и на Западе, которые также характеризуют динамику подвергающеюся атакам общественного мнения.

По этим данным можно судить о состоянии общества, атакуемого деструктивными контентами и технологиями, включая – прогнозирование перспектив реализации рассматриваемых угроз [3-6].

Важнейшим вопросом исследования являются атакующие средства, многообразие которых достаточно полно должно быть рассмотрено и классифицировано. К примеру, для вредоносных контентов часто применяется их тематическая классификация и оценка частоты их вбросов в социо-информационное пространство. При этом одним из классификационных признаков уместно использовать тип источника угроз.

Анализ не будет полным, если исследователь не рассматривает ареалы атакуемых объектов и влияние на них деструктивного контента.

Основную практическую ценность исследования прежде всего представляют средства управления рисками. Их классификация осуществляется по масштабности (надгосударственные, государственные, корпоративные и личные), профильности (организационно-правовые, технические и др.) и прочим признакам. Исследователь должен внести свои предложения по всем разновидностям управления, указав проектные ситуации для их наиболее эффективного применения. Рекомендации автора обязаны отличаться практической конкретностью (рис. 1).

Относительно списка литературы следует заметить, что он не должен состоять лишь из русскоязычных источников. Отход от этой однобокости существенно обогатит работу. Чрезмерное цитирование интернет-источников, где изобилуют отнюдь не научные и зачастую жаргонные тексты, также не приветствуются. При этом необходимо следить за оригинальностью работы (уважающие себя исследователи не допускают её значение менее 85%), поэтому все цитаты снабжаются ссылками. Формулировка работы отражает объекты и предмет исследования в рамках рассматриваемой проблемы, которая в нашей профессии относится к информационному пространству, атакуемому, по большому счету, двумя типами боеголовок: вредоносный код и деструктивный контент. При этом наша профессиональная задача состоит в управлении информационными рисками, минимизируя их и минимизируя шансы устойчивого развития для объекта исследования (рис. 2).

Методические рекомендации

Актуальность темы обосновывается на основе подробного анализа литературных источников, исключительно по тематике исследования.

Противоречия обычно существуют между необходимостью получения неких новых качеств в объекте исследования и полным либо частичным отсутствием средств их достижения в аналогах

Разрешение противоречия достигается решением соответствующей ему задачи. Имеют место быть противоречия между необходимостью адекватной оценки рисков успешной реализации атак на объект исследования и способностью существующего методического и др. обеспечения для решения этого класса задач.

Цель исследования (одной фразой формулируется достижение, которое планирует получить автор, в результате решения поставленных задач). У нас это обычно – повышение защищенности от угроз.

Базой для постановки задач служит первая глава ВКР, где не нужен «ликбез», а требуется детальное исследование аналогов и выявление в них противоречий, каждому из которых взаимно однозначно соответствует задача, конкретно и четко сформулированная.

Каждой задаче взаимно однозначно должен соответствовать не процесс, а результат, новизна, практическая ценность и теоретическая значимость которого обязательно оцениваются.

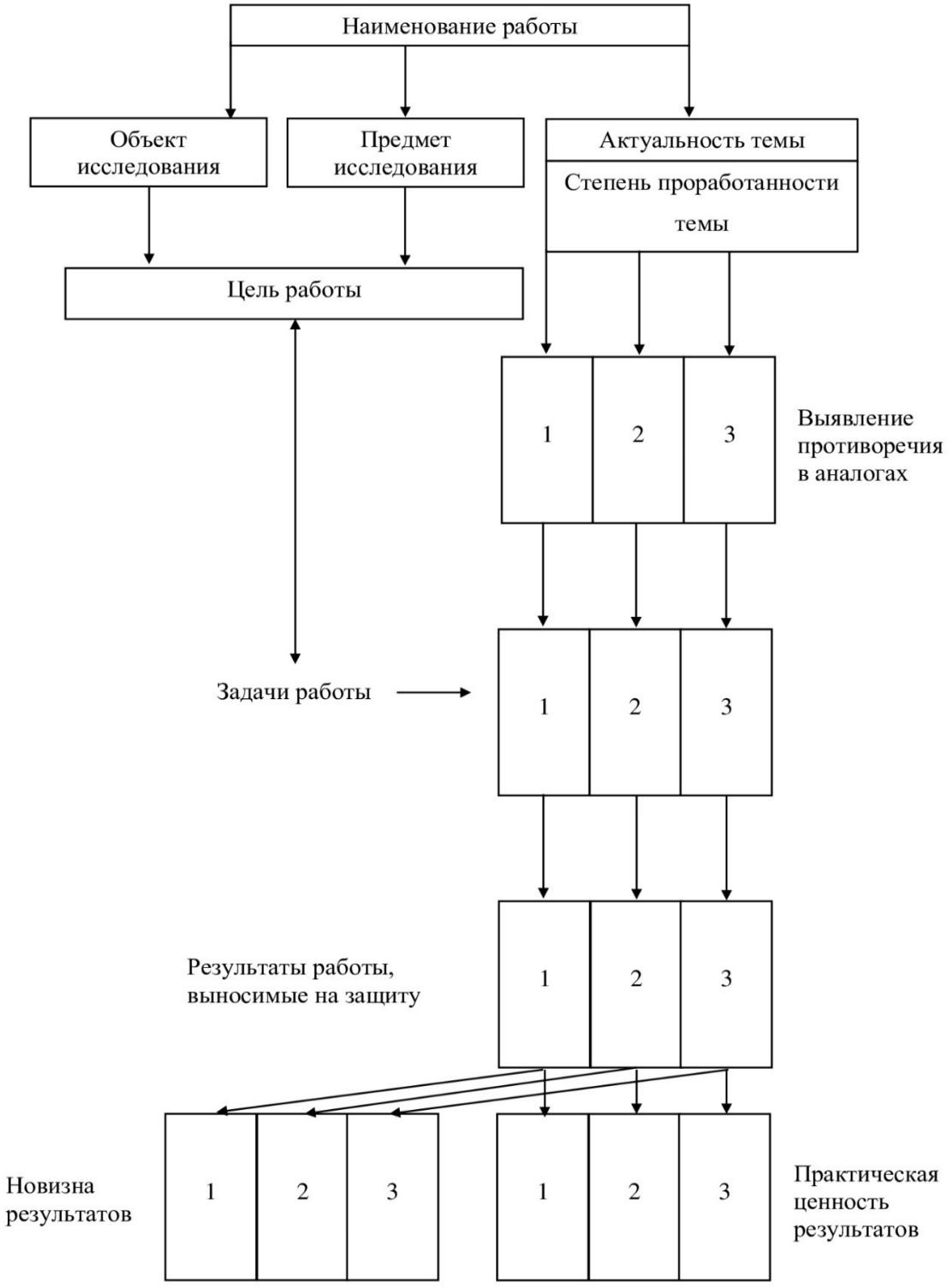

Рис. 2. Схема построения ВКР по принципу сквозного соответствия элементов (противоречие – задача – результат – его новизна и практическая ценность)

Работа считается незаконченной, если в ней отсутствует аналитическая оценка повышения защищенности объекта в результате применения полученных автором результатов.

Перечень защищаемых объектов и угроз должен быть четко определен. **Невозможно** защищать все системы от всевозможных угроз (определяющим здесь является информационное обеспечение, доступное в рамках подготовки ВКР).

Оценка эффективности результатов должна быть численной и масштабной для объекта и предмета исследования. Фальсификация данных здесь недопустима!

Предложенные в рамках проектирования методики и полученные алгоритмические (технические) решения составляют теоретическую значимость результатов, в то время как практическую ценность результатов имеют созданные дополнения к программно-техническим комплексам и предложенные в ходе подготовки ВКР методики (устройства) снижения рисков.

Выносимые на защиту результаты. Для каждой поставленной задачи персонально и подробно раскрывается ожидаемый результат исследования.

Календарное планирование

Важнейшее практическое значение имеет график дипломного проектирования. Ниже приводится пример такого документа (табл. 1), который обеспечивает требуемую последовательность и ритмичность подготовки ВКР. Иллюстрация (табл. 1) ориентирована на хронологию методики-алгоритмы-программы. Однако, она может быть легко адаптирована для триады методики-структуры-устройства, которая также имеет место быть при технической защите информации. Предлагаемый график (табл. 1) также синхронизирован с нормативом преддипломной практики. Для выдающихся ВКР он открывает возможность публикации и внедрения результатов с использованием возможностей выпускающей кафедры и её базовых предприятий.

Таблица 1

Пример графика дипломного проектирования

№	Этапы проектирования	Сроки отчетности
1.	Введение и литература. Глава 1. Исследование аналогов и постановка задач работы	28 февраля 2022 г.
2.	Глава 2. Методическое обеспечение противодействия угрозам	31 марта 2022 г.
3.	Глава 3. Алгоритмическое обеспечение противодействия угрозам	30 апреля 2022 г.
4.	Глава 4. Программное обеспечение противодействия угрозам	31 мая 2022 г.
5.	Отчет по преддипломной практике, уточнение формулировок тем и допуск к защите	31 мая 2022 г.
6.	Подготовка проекта публикации (для выдающихся работ)	16 мая 2022 г.
7.	Отладка, тестирование, оценка эффективности и внедрение защищаемого продукта	10 июня 2022 г.
8.	Приложения. Описание продукта и практические рекомендации по противодействию угрозам	13 июня 2022 г.
9.	Оформление, проверка оригинальности, нормоконтроль, рецензирование ВКР	27 июня 2022 г.
10.	Защита ВКР	7 июля 2022 г.

Даты, представленные в примере, носят условный характер и для специальностей со сроком обучения 5,5 лет должны быть скорректированы под осенний семестр.

Заключение

По большому счету:

1. Входное целеполагание ВКР должно опираться на деревья угроз и рисков, где достаточно полно представлены опасности, подстерегающие объект исследования в информационной сфере.

2. Далее интересует аналитическая оценка выявленных рисков в динамике реализации угроз (в этом случае становится очевидным увеличение или снижение опасности в условиях применения тех или иных мер противодействия угрозам).

3. Наконец, выпускник обязан в ВКР выработать предложения (рекомендации) практического плана по снижению величины выявленных рисков и парирования угроз для объекта исследования.

Список литературы

1. Эпидемии в телекоммуникационных сетях : монография / А.Г. Остапенко [и др.] ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 1. М. : Горячая линия-Телеком, 2017. 282 с.

2. Атакуемые взвешенные сети : монография / А.Г. Остапенко [и др.] ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 2. М. : Горячая линия-Телеком, 2017. 248 с.

3. Социальные сети и деструктивный контент : монография / А.Г. Остапенко [и др.] ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 3. М. : Горячая линия-Телеком, 2017. 274 с.

4. Социальные сети и риск-мониторинг : монография / А.Г. Остапенко [и др.] ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 4. М. : Горячая линия-Телеком, 2020. 266 с.

5. Социальные сети и психологическая безопасность : учеб. пособие для вузов / А.Г. Остапенко [и др.] ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 5. М. : Горячая линия-Телеком, 2021. 266 с.

6. Сетео-информационная эпидемиология : учеб. пособие для вузов / А.Г. Остапенко [и др.] ; под ред. Д.А. Новикова ; серия «Теория сетевых войн» ; вып. 6. М. : Горячая линия-Телеком, 2021. 216 с.

7. ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности. https://docs.cntd.ru/document/1200084141 (дата обращения 10.03.2022).

8. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации. https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377- (дата обращения 10.03.2022).

9. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности https://docs.cntd.ru/document/1200112881 (дата обращения 10.03.2022).

Воронежский государственный технический университет
Voronezh State Technical University

Воронежский государственный аграрный университет имени императора Петра I
Voronezh State Agrarian University named after Emperor Peter I

Поступила в редакцию 15.03.2022

Информация об авторах

Разинкин Константин Александрович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Кострова Вера Николаевна – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Питолин Владимир Михайлович – д-р техн. наук, профессор, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Соколова Елена Сергеевна – ассистент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Нархов Дмитрий Андреевич – студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

Прохорова Алёна Евгеньевна – студентка, Воронежский государственный аграрный университет имени императора Петра I, e-mail: alena_prokh@mail.ru

SPECIALTY "INFORMATION SECURITY": BRIEF SCIENTIFIC AND METHODOLOGICAL RECOMMENDATIONS FOR THE PREPARATION OF FINAL QUALIFYING WORKS

K.A. Razinkin, V.N. Kostrova, V.M. Pitolin, E.S. Sokolova, D. A. Narhov, A.E. Prokhorova

The article describes the main scientific and methodological recommendations for the preparation of final qualifying papers. The basic terminology that is used during the diploma design and the features of the classified tree that contributes to the fundamental analysis of threats and risks are announced. The points are listed (in the context of the study), the main idea of which is the inadmissibility of using information that does not have a sufficiently powerful theoretical and evidence base. Recommendations for the preparation of the final qualifying work are prescribed. The work is focused on the specialties "Information security of telecommunication systems", "Information security of automated systems" and "Computer security". The proposals formulated in it take into account the experience of preparing and defending the final qualifying work in the above specialties, which has developed at the Voronezh State Technical University. The rapid increase in the multitude and danger of information risks generated by the revolutionary digital transformation of the individual, society and the state determines the practical relevance of the scientific and methodological recommendations of this work for graduate students, their supervisors and graduates of the departments of the specialty "Information Security".

Keywords: risk, threats, final qualifying work, analytical assessment, object and subject of research, contradictions, results.

Submitted 15.03.2022

Information about the authors

Konstantin A. Razinkin – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

Vera N. Kostrova – Dr. Sc. (Technical), Professor, Voronezh State Technical University, e-mail: mnac@comch.ru

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

Elena S. Sokolova – Assistant, Voronezh State Technical University, e-mail: mnac@comch.ru

Dmitry A. Narhov – **S**tudent, Voronezh State Technical University, e-mail: mnac@comch.ru

Alyona E. Prokhorova –Student, Voronezh State Agrarian University named after Emperor Peter I, e-mail: alena_prokh@mail.ru