МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ МЕЖДУНАРОДНЫХ ОТНОШЕНИЙ
Кафедра международных отношений

Аннотация к магистерской диссертации

ПРОТИВОДЕЙСТВИЕ ФРГ УГРОЗАМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В НАЧАЛЕ XXI в.

Войтова Виктория Сергеевна

Научный руководитель - доктор исторических наук, профессор М.Э.Чесновский

Минск, 2017

АННОТАЦИЯ

1. Структура и объем магистерской диссертации

Диссертация состоит из перечня условных обозначений, общей характеристики работы, введения, четырех глав, заключения, библиографического списка. В главах диссертации отражены особенности противодействия ФРГ угрозам информационной безопасности в начале XXI в.

Полный объем диссертации составляет 80 страниц, библиографический список из 94 наименований занимает 9 страниц.

2. Перечень ключевых слов

ФРГ (ГЕРМАНИЯ), ЕС, НАТО, США, КИБЕРБЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ (ИКТ), КИБЕРПРОСТРАНСТВО, КИБЕРПРЕСТУПНОСТЬ, КИБЕРТЕРРОРИЗМ.

3. Содержание работы

Объектом исследования является обеспечение информационной безопасности ФРГ и ее союзников.

Цель исследования – показать, что на стыке развития информационно-коммуникационных технологий и обеспечения национальной безопасности ФРГ в начале XXI в. оказалась обостряющаяся проблема кибертерроризма.

Методы исследования. В работе использован междисциплинарный подход, совмещающий исторический и политологический анализ, а также методы сравнительного и контекстуального анализа.

Полученные итоги и их новизна. Научная новизна исследования заключается в том, работа является одной из первых в белорусской историографии попыток системного исследования проблемы кибертерроризма и политики ФРГ по противодействию ему. Практическая новизна работы заключается в возможности использования ее результатов при изучении политики противодействия угрозам информационной безопасности других европейских государств, в том числе, Республики Беларусь.

Достоверность материалов и результатов магистерской диссертации. Использованные материалы и результаты магистерской диссертации являются достоверными. Работа выполнена самостоятельно.

Рекомендации по использованию результатов работы. Работа может представлять интерес для педагогических, научных и дипломатических работников, занимающихся вопросами информационной безопасности и кибертерроризма.

АНАТАЦЫЯ

1. Структура і аб’ём магістэрскай дэсертацыі

Дысертацыя складаецца з пераліку ўмоўных скарачэнняў, агульнай характарыстыкі працы, уводзінаў, чатырох глаў, заключэння, бібліяграфічнага спісу. У раздзелах дысертацыі адлюстраваны асаблівасці процідзеяння ФРГ пагрозам інфармацыйнай бяспекі ў пачатку XXI ст.

Поўны аб'ём дысертацыі складае 80 старонак, бібліяграфічны спіс з 94 найменняў займае 9 старонак.

2. Пералік ключавых слоў

ГЕРМАНІЯ, ЕЎРАПЕЙСКІ САЮЗ, НАТО, ЗША, КІБЕРБЯСПЕКА, ІНФАРМАЦЫЙНАЯ БЯСПЕКА, ІНФАРМАЦЫЙНА-КАМУНІКАЦЫЙНЫЯ ТЭХАЛОГІІ (ІКТ), КІБЕРПРАСТОРА, КІБЕРЗЛАЧЫННАСЦЬ, КІБЕРТЭРАРЫЗМ.

3. Змест працы

Аб'ектам даследавання з'яўляецца забеспячэнне інфармацыйнай бяспекі ФРГ і яе саюзнікаў.

Мэта даследвання – паказаць, што на сутыку развіцця інфармацыйна-камунікацыйных тэхналогій і забеспячэння нацыянальнай бяспекі ФРГ у пачатку XXI ст. апынулася праблема кібертэрарызму.

Метады даследавання. У працы выкарыстаны міждысцыплінарны падыход, які сумяшчае гістарычны і паліталагічны аналіз, а таксама метады параўнальнага і кантэкстуальнага аналізу.

*Атрыманыя вынікі і іх навізна***.** Навуковая навізна даследавання заключаецца ў тым, што праца з'яўляецца адной з першых у беларускай гістарыяграфіі спроб сістэмнага даследавання праблемы кібертэрарызму і палітыкі ФРГ па супрацьдзеянні яму. Практычная навізна працы заключаецца ў магчымасці выкарыстання яе вынікаў пры вывучэнні палітыкі процідзеяння пагрозам інфармацыйнай бяспецы іншых еўрапейскіх дзяржаў, у тым ліку Рэспублікі Беларусь.

*Дакладнасць матэрыялаў і вынікаў магістэрскай дысертацыі***.** Выкарыстаныя матэрыялы і вынікі магістэрскай дысертацыі з’яўляюцца дакладнымі. Праца выканана самастойна.

Рэкамендацыі па выкарыстанні вынікаў працы. Праца можа прадстаўляць інтарэс для педагагічных, навуковых і дыпламатычных работнікаў, якія займаюца пытаннямі інфармацыйнай бяспекі і кібертэрарызму.

ANNOTATION

1. Structure and scope of the master's thesis

The thesis consists of a list of abbreviations, a general description of the work, introduction, four chapters, conclusion and a bibliographic list. Tthesis's chapters reflect the features of Germany's counteraction with information security threats in the early 21st century.

The full volume of the thesis is 80 pages, the bibliographic list of 94 titles covers 9 pages.

2. Key words

FEDERAL REPUBLIC OF GERMANY, THE EUROPEAN UNION, NATO, USA, CYBER SECURITY, INFORMATION SECURITY, INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT), CYBERSPACE, CYBERCRIME, CYBERTERRORISM.

3. The context of the work

The object of research is ensuring Germany's and its allies information security.

The purpose of the research is to show that an escalating problem of cyberterrorism ended up at the junction of the development of information and communication technologies and ensuring Germany's national security at the beginning of the 21st century.

Methods of research. The author used a multidisciplinary approach, combining historical and political analysis as well as methods of comparative and contextual analysis.

The results of the work and their novelty. The scientific novelty of the study lies within the fact that the work is one of the first attempts in belarusian historiography to make a comprehensive study of the cyberterrorism problem and Germany's policy of dealing with it. The practical novelty of the work lies in the possibility of using its results while studying the policy of countering information security threats in other European states.

Authenticity of the materials and results of the master's thesis. The materials used and the results of the master's thesis are authentic. The work has been put through independently.

Recommendations on the usage. The work may be of interest to teachers, scientists and diplomats, who work with issues in information security and cyberterrorism.