МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное
учреждение высшего образования
«Воронежский государственный технический университет»

Кафедра систем информационной безопасности

ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению курсовой работы
для студентов специальностей
10.05.01 «Компьютерная безопасность»
10.05.02 «Информационная безопасность телекоммуникационных систем»
10.05.03 «Информационная безопасность автоматизированных систем»
очной формы обучения

Воронеж 2023

УДК 004.057:004.735

Составители:
д-р техн. наук А.Г. Остапенко
студент Д.А. Нархов
студент А.Ю. Егоров
аспирант Н М. Лантюхов
студент А.А. Остапенко

Введение в специальность: методические указания к выполнению курсовой работы для студентов специальностей 10.05.01 «Компьютерная безопасность» 10.05.02 «Информационная безопасность телекоммуникационных систем» 10.05.03 «Информационная безопасность автоматизированных систем» / ФГБОУ ВО «Воронежский государственный технический университет»; сост.: А.Г. Остапенко, Д.А. Нархов, А.Ю. Егоров, Н.М. Лантюхов – Воронеж: Изд-во ВГТУ, 2023. – 24 с.

Методические указания разработаны с целью организации процессов подготовки и защиты курсовой роботы обучающихся по дисциплине «Введение в специальность». В рекомендациях определены требования к содержанию и структуре работы, основные направления деятельности обучающихся и руководителя работы.

Предназначены для студентов специальностей 10.05.01 «Компьютерная безопасность» 10.05.02 «Информационная безопасность телекоммуникационных систем» 10.05.03 «Информационная безопасность автоматизированных систем» всех форм обучения.

Подготовлены в электронном виде и содержатся в файле МУ_КУР_ВВС_2023.pdf.

Ил. 6. Табл. 6. Библиогр.: 6 назв.

УДК 004.057:004.735

Рецензент – К.А. Разинкин д-р технических наук, профессор кафедры систем информационной безопасности ВГТУ

Издается по решению редакционно-издательского совета Воронежского государственного университета

СОДЕРЖАНИЕ

ГЛОССАРИЙ 3
ВВЕДЕНИЕ 4
1 Рекомендуемые структура, цель и задачи курсовой работы 6
1.1 Общие требования 6
1.2 Структура курсовой работы 6
2 Методическое обеспечение для классификации контентов, циркулирующих в интернет-ресурсе 9
2.1 Структурно-функциональная специфика исследуемого сервиса 9
2.2 Тематическая классификация циркулирующего контента 10
3 Методическое обеспечение для проведения риск-анализа контентов, циркулирующих в интернет-ресурсе 14
3.1 Качественный анализ угроз воздействия деструктивного контента 14
3.2 Параметры метрологии контентов 15
3.3 Базовые метрики контент-мониторинга 17
3.4 Оценка рисков 19
4 Меры противодействия распространению деструктивного контента 21
ЗАКЛЮЧЕНИЕ 23
СПИСОК ЛИТЕРАТУРЫ 24

ГЛОССАРИЙ

Таблица 1

Глоссарий терминов, используемых в курсовой работе

Термин	Определение термина
Социальная сеть	Интернет-площадка, сайт, который позволяет зарегистрированным на нем пользователям размещать информацию о себе и коммуницировать между собой
Пользователь сети	Конкретное лицо, которое входит в интернет-пространство и использует действующую систему для выполнения конкретных задач или функций
Контент сети	Информационно значимое наполнение ресурса социальной сети
Деструктивный контент	Контент с признаками деструктивности, определёнными действующим законодательством РФ
Угроза пользователям сети	Процессы распространения и восприятия в сети деструктивных контентов
Ущерб	Множество пользователей, позитивно отреагировавших на деструктивный контент
Риск	Возможность невиртуальных деструктивных действий пользователей сети, одобривших деструктивный контент
Безопасность	Состояние множества пользователей сети, при котором риск не превышает допустимого уровня
Лайк	Выражение первичного одобрения контента
Просмотр	Количество просмотров публикации с момента публикации контента
Дизлайк	Выражение неодобрения материалу или пользователю
Репост	Выражение желания поделиться контентом с другими пользователями
Комментарий	Развернутое выражение одобрения или неодобрения контента через комментирование его содержания
Мониторинг контентов	Измерение и контроль параметров контента в период его жизни
Шаг мониторинга	Период повторения отсчетов мониторинга контента во время его жизни
Время жизни контента	Период времени от возникновения контента до потери им своей популярности
Период роста популярности контента	Период времени, когда количество просмотров растет и достигает своего максимума
Период спада популярности контента	Период, когда, достигнув своего максимума, популярность контента у пользователей сети спадает

ВВЕДЕНИЕ

Информационное пространство в силу его глобальности не имеет государственных границ, и поэтому нередко оно используется для вторжений в личную жизнь граждан и общественную деятельность социумов, так как за циркуляцией в нём контент-трафика практически невозможно уследить. Дело в том, что в этом многослойном и мультиразмерном пространстве нет всеобщей цензуры. Этот факт открывает широкие возможности для злоумышленников, специальных служб разных стран мира, а также террористических организаций. Причем наибольший интерес для них представляют социальные сети, охватывающие в своем информационном пространстве едва ли не треть человечества. Здесь им открываются практически безграничные возможности для информационно-психологического воздействия на пользователей сети. В результате социальные сети стали ареной не только для недобросовестной конкуренции, но и откровенного информационного противоборства, в котором активно участвуют и государственные структуры. Руководители ведущих стран прекрасно понимают, что от того, как выглядит их политика в социальных сетях, во многом зависят общественное мнение и поддержка населения. Мало того, проигрыш в информационно-психологическом пространстве может привести к утрате власти и политического влияния не только отдельного руководителя, но и целых стран.

Социальные сети – сегодня самый мощный вещатель. Пользователь – субъект сети, объективно заинтересованный в достижении максимальной популярности в социуме и в получении самой полезной информации через сетевые сервисы. В этом состоит феномен лавинообразного роста количества соцмедиа различного назначения и их пользователей, а также - ожесточенной конкурентной борьбы в этом информационном пространстве. Фактически речь идет о битве контентов за информационно-психологические предпочтения массы социально и экономически активных людей, охватывающей треть человечества. Ставки весьма высоки, и поэтому технологическая изощрённость конструирования и распространения контента в социальных сетях превышает всякие ожидания. Существует противоречивое отношение к информации в интернет-сфере: с одной стороны, многие граждане пользуются различными интернет-услугами, социальными сетями для общения, обмена аудио- и медиаконтентом, с другой стороны, по причине отсутствия действенных механизмов регулирования информационного взаимодействия доверие к информации, размещенной в сети Интернет, часто не высокое.

Важность информационной сферы подтверждают слова В.В. Путина на заседании Совета Безопасности РФ от 26.10.17 «Следует повысить безопасность и устойчивость работы инфраструктуры российского сегмента интернета… Как и в других демократических странах, мы должны бороться с теми, кто использует информационное пространство для пропаганды

радикальных идей, оправдания терроризма, экстремизма, решительно пресекать попытки размещения материалов, угрожающих безопасности нашего государства, общества в целом и отдельных граждан».

Одно из центральных мест в этом направлении занимает борьба с деструктивным контентом и его негативным влиянием на граждан Российской Федерации, которое является основным оружием информационно-психологических войн (операций) и наносит серьёзный ущерб государству. Поэтому это влияние является предметом пристального внимания как специалистов в области информационно-психологических операций (войн), так и тех, кто призван обеспечивать информационно-психологическую безопасность личности, общества и государства. Например, в начале 2011 года волна манифестаций, а за ними и политических переворотов охватила практически всю Северную Африку и Ближний Восток. События разворачивались по одному и тому же сценарию. Несколько десятков молодых людей создавали в социальной сети группу недовольных действиями политических властей, договаривались в ней о проведении уличной акции протеста, чаще всего, демонстрации с антиправительственными лозунгами. Такая демонстрация в жесткой форме, т.е. с применением спецсредств, разгонялась полицией, а небольшая группа бунтарей оказывалась под арестом. Но видео, фотографии, сообщения о разгоне демонстрации начинали активно распространяться в сети с призывом выйти на улицы более многочисленной и сплоченной группой. Так единичные и малочисленные акции протеста приводили к многотысячным и многодневным манифестациям и даже – «цветным революциям».

Неудивительно, что в ходе реализации Специальной военной операции Вооруженных сил Российской Федерации на Украине, социальные сети стали активно использоваться для информационного противоборства. Грязная русофобия и даже призывы уничтожить россиян потоком хлынули в отечественное социо-информационное пространство из бендеровских рупоров пропаганды.

Таким образом, в связи с высокой популярностью социальных сетей они помимо выполнения функций поддержки общения, обмена мнениями и получения информации всё чаще становятся средствами информационного управления, а также ареной информационного противоборства. Они являются существенным инструментом информационного влияния, в том числе – в целях манипулирования личностью, социальными группами и обществом в целом, а также полем информационной войны.

Всё вышеизложенное обуславливает объективную необходимость мониторинга безопасности социальных сетей, чему собственно и посвящена настоящая курсовая работа.

1 Рекомендуемые структура, цель и задачи курсовой работы

1.1 Общие требования

В рамках курсового проектирования студентам предлагается провести самостоятельное исследование, в результате которого будущие специалисты приобретают навыки работы с научной и методической литературой, а также - со специализированными программными комплексами.

Объектом исследования выступают интернет-ресурсы, в которых циркулируют деструктивные контенты.

В этом контексте для специальностей 10.05.01 «Компьютерная безопасность (КБ)», 10.05.02 «Информационная безопасность телекоммуникационных систем (БТ)», 10.05.03 «Информационная безопасность автоматизированных систем (ИБ)» следует исходить из анализа угроз объекту исследования и через оценку рисков их реализации предложить риск-управление в интересах обеспечения информационной безопасности (ИБ) личности, общества и государства.

1.2 Структура курсовой работы

Курсовая работа оформляется в соответствии с общими правилами оформления научно-исследовательских работ и содержит:

а) титульный лист;

б) задание на курсовую работу;

в) лист «Замечания руководителя»;

г) содержание, которое включает введение, наименование всех разделов, подразделов, пунктов (если они имеют наименование), заключение, список литературы, приложения (при необходимости);

д) глоссарий;

е) введение;

ж) основную часть;

з) заключение;

и) список литературы;

к) приложения (при необходимости).

Объем курсовой работы составляет 30-50 страниц без приложений, списка литературы и глоссария.

Введение отражает актуальность и логику проведенного исследования, через систему целеполагания и позволяет оценить степень разработанности выбранной темы.

Введение должно содержать следующие пункты:

• обоснование выбранной темы в рамках дисциплины;

• основную цель и задачи работы;

• объект и предмет исследования.

Обоснование выбора темы и ее актуальность должна касаться непосредственно выбранной темы исследования. Актуальность темы — это та

причина, по которой именно сейчас, в настоящее время, возникла потребность в данном исследовании. Не рекомендуется при обосновании актуальности приводить общие формулировки, не относящиеся непосредственно к выбранной теме исследования.

Объектом исследования является региональное интернет-сообщество.

Предмет исследования – оценка риска вовлеченности пользователей социо-информационного пространства в деструктивный контент.

Целью работы является повышение защищенности пользователей социо-информационного пространства от угроз, порождаемых деструктивным контентом, за счет риск-анализа процессов его распространения и восприятия и выработки рекомендаций по противодействию деструктивам.

Для достижения поставленной цели необходимо выполнить следующие задачи:

1. выявление в интернет-ресурсе и классификация контентов с признаками деструктивности;
2. риск-анализ интернет-ресурса и циркулирующих в нём деструктивных контентов;
3. выработка рекомендаций по противодействию деструктивным контентам в исследуемом интернет-ресурсе.

Основная часть должна содержать следующие подразделы:

1) исследование интернет-ресурса:

1.1) описание исследуемого ресурса;

1.2) структурно-функциональная специфика интернет-сообщества;

1.3) качественный и количественный состав пользователь (портрет пользователя интернет-сообщества);

1.4) классификация деструктивного контента, циркулирующего в интернет-сообществе.

2) риск-анализ процессов распространения и восприятия деструктивного контента:

2.1) качественный анализ рисков, индуцированных угрозой воздействия деструктивного контента;

2.2) определение объектов и измеряемых параметров метрологии;

2.3) измерение базовых метрик контент-мониторинга;

2.4) количественная оценка риска вовлеченности пользователей интернет-ресурса в деструктивный контент.

3) выработка рекомендаций по противодействию деструктивным контентам в исследуемом интернет-ресурсе.

На защиту выносятся следующие результаты:

1. совокупность выявленных в интернет-ресурсе деструктивных контентов, их классификация;
2. риски вовлеченности пользователей ресурса в содержание тематического деструктивного контента;
3. совокупность рекомендаций по противодействию распространению деструктивного контента в исследуемом интернет-ресурсе.

В заключении курсовой работы отражаются следующие аспекты:

• сжатая формулировка основных выводов, вытекающих из результатов проведенного исследования;

• предложения по развитию проведенного исследования в целях повышения защищенности регионального социо-информационного пространства.

Выводы – умозаключения, сделанные на основе анализа теоретического и/или эмпирического материала.

Количество выводов может быть разным, однако должно составлять не менее 3–5. При большем их количестве желательно вводить в перечень выводов дополнительное структурирование, т.е. разбивать их на группы по некоторому логическому основанию.

Выводы должны содержать оценку соответствия результатов поставленным целям, задачам и проблеме исследования.

После заключения располагается список литературы. На каждый источник обязательно должна быть ссылка в тексте. Количество использованных источников свидетельствует о глубине проработанности поставленной проблемы. Список литературы должен состоять не менее чем из 10 наименований монографических работ, научных статей. Также необходимо использование монографий серии «Теория сетевых войн» [1-4] и статей научного журнала «Информация и безопасность» [5-6].

Приложения располагают после списка литературы. Их цель – избежать излишней нагрузки текста различными аналитическими, расчетными, статистическими материалами, которые не содержат основную информацию. Каждое приложение начинается с новой страницы и имеет заголовок.

2 Методическое обеспечение для классификации контентов, циркулирующих в интернет-ресурсе

2.1 Структурно-функциональная специфика исследуемого сервиса

Всех субъектов сообщества целесообразно разделить на два основных типа: авторизованные и неавторизованные пользователи. Классификация субъектов сети представлена на рисунке 1.

К первому типу относятся легитимные пользователи, фейковые аккаунты и социальные боты. Легитимные пользователи в свою очередь подразделяются на привилегированных пользователей и обычных. К привилегированным пользователям относятся пользователи, которые имеют большие возможности в социальной сети, чем другие. Например, к таким пользователям относятся администраторы, модераторы, редакторы. Администраторы наделены всеми правами модератора и редактора, они отвечают за управление сообществами, могут назначать и удалять руководителей сообществ, редактировать любую информацию о сообществах. Модераторы следят за порядком в сообществах и обладают возможностями редактирования контента в сообществах.

К неавторизованным пользователям стоит отнести удаленные и замороженные аккаунты. Каждый пользователь может по собственному желанию удалить собственную страницу из социальной сети.

В случае если пользователь захочет восстановить удаленный аккаунт, то в течение 7 месяцев с момента удаления он может это сделать без потери всех данных. Заморозка страницы ВКонтакте может произойти, если пользователь будет замечен за подозрительной активностью, например, в рассылке спама в публичной странице. Субъекты публичной страницы (группы) изображены на рисунке 1

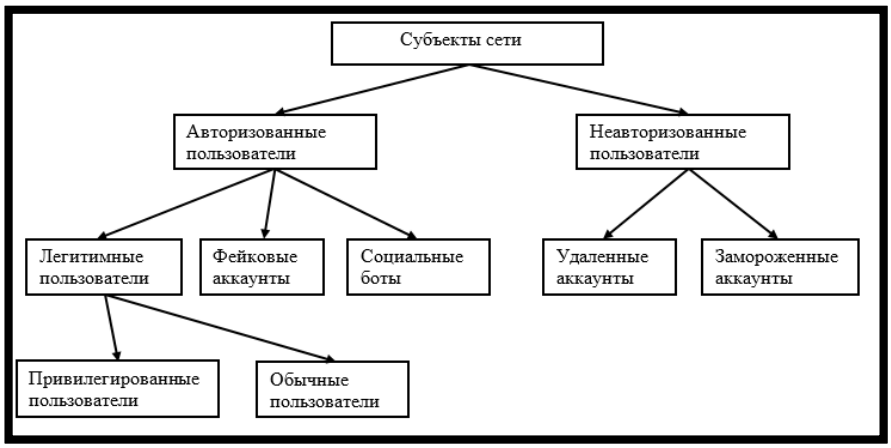

Рис. 1 Классификация субъектов в группе

Фейковые аккаунты могут использоваться для распространения различной рода информации. Зачастую бывает достаточно трудно отличить фейковый аккаунт от легитимного пользователя.

2.2 Тематическая классификация циркулирующего контента

Для контента характерны две ключевые характеристики: уникальность и логическое построение [1].

Уникальный контент – это самостоятельный аутентичный текст, функционирующий в реальной науке, разработанный содружеством ученых, вносящих свой вклад в контент научной дисциплины. Понятие «уникальный контент» подразумевает одинаковость структуры и содержания информационной составляющей данной научной дисциплины.

Неуникальный контент – это текст, который был скопирован (из книг, сайтов и прочих источников, уже реально использованных в данной научной дисциплине).

Отсутствие логического построения контента делает его непригодным для использования. Прогрессивное развитие информационных интернет-ресурсов привело к появлению разных видов контента (рис.2) [1].

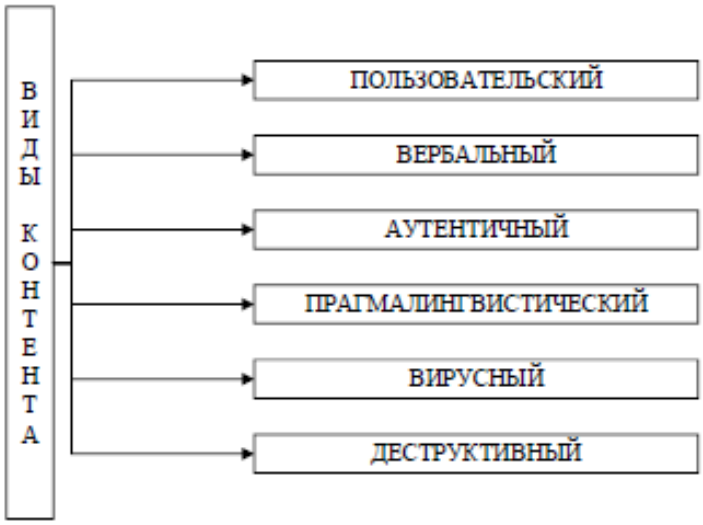

Рис. 2 Классификация разновидности контента

Открытый контент (open content) – неологизм, возникший по аналогии с open source, описывает любое творческое произведение или контент, опубликованный под лицензией, которая явно разрешает копирование и изменение этой информации кем угодно, а не только закрытой организацией, фирмой или частным лицом. Открытый контент способствует целям демократизации знаний. Крупнейшим проектом open content является Википедия.

Пользовательский контент (UGC – user generated content) – это оригинальный контент, который создается аудиторией определенного интернет-ресурса. Этим контентом может быть все что угодно – начиная с отзывов и комментариев в блоге и заканчивая фото- и видеороликами.

Вербальный контент – словесная конструкция для передачи информации. Невербальный контент – прагматически обусловленный содержательный компонент контента, несущий большую долю фактической информации и вносящий определенный вклад в создание ее композиционно-смыслового единства.

Аутентичный контент – оригинальный материал, взятый из подлинных источников и не предназначенный первоначально для учебных целей.

Прагмалингвистический контент – учебный контент на основе преобразованного в образовательных целях аутентичного оригинального контента.

Вирусный контент – это информация, распространяющаяся по сети Интернет с прогрессирующей скоростью посредством передачи от пользователя к пользователю (по принципу «сарафанного радио»). Это контент, созданный по приемам вирусного маркетинга и состоящий из ярких, неординарных, срочных, эмоциональных, интересных и захватывающих внимание материалов, которыми добровольно делится аудитория.

В распространении вирусного контента участвуют получатели материалов, которые сами и вовлекают в «вирусный процесс» новых участников.

Графический контент – это изображения. Ими могут быть разные виды фотографий (простые, 3-D, панорамные), графические иллюстрации, рисунки, таблицы, диаграммы и графики, анимация и инфографика. Изображения воздействуют на образное мышление и облегчают восприятие текстовой информации, помогают для понимания выделить нужное и делают любую веб-страницу наглядней и интересней. А инфографика вообще способна заменить текст.

Видеоконтент – это некая информация, представленная в мультимедийном формате, которая создается под потребности и интересы целевой аудитории. Иными словами, это видеозапись, которая пользуется спросом у пользователей, поскольку имеет для них какую-то ценность.

Деструктивный контент – информация, воплощающая в своем содержании негативную оценку конкретного лица, социальной группы, связей и отношений с ними, в том числе через обесценивание характеристик, призывы к уничтожению.

Классифицируют деструктивный контент по следующим признакам [2]:

1) разжигание этнической и религиозной ненависти. Данное направление соответствует статьей 282 УК РФ «Возбуждение ненависти либо вражды, а равно унижение человеческого достоинства», также статье 29 Конституции Российской Федерации, где говорится, что «не допускаются пропаганда или агитация, возбуждающие социальную, расовую, национальную или религиозную ненависть, или вражду». Данная статья призвана служить пропаганде толерантности по отношению к других национальным (социальным) группам и сообществам. Согласно Доктрине информационной безопасности Российской Федерации (утв. Указом

Президента Российской Федерации от 5 декабря 2016 г. №646), которая является основополагающим документом в области информационной безопасности, уделяется большое внимание действиям в интернет-пространстве, направленным на «разжигание этнической и религиозной ненависти либо вражды» по отношению к отдельным этносам, религиозным группам, народам и национальностям. Зачастую, такой деструктивный контент представляет собой видеоматериалы пропагандистского типа, которые показывают определенную группу населения в негативном ключе, побуждая к активным действиям, направленным против такой категории людей.

2) пропаганда экстремизма. Данное направление регулируется следующими правовыми актами: КоАП РФ Статья 20.3. «Пропаганда либо публичное демонстрирование нацистской атрибутики или символики, либо атрибутики или символики экстремистских организаций, либо иных атрибутики или символики, пропаганда либо публичное демонстрирование которых запрещены федеральными законами»; УК РФ Статья 280. «Публичные призывы к осуществлению экстремистской деятельности», которая ссылается на статью 1 федерального закона "О противодействии экстремистской деятельности", где раскрывается понятие «экстремизма». Данное направление является одним из наиболее важных, так как последствия пропаганды экстремизма объективно являются особенно опасными для современного общества.

3) пропаганда наркотиков. Данное направление деструктивного контента определяется статьей 230 УК РФ «Склонение к потреблению наркотических средств, психотропных веществ или их аналогов», статьей 4 Федерального закона «О средствах массовой информации», статьей 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию». Часто такой деструктивный контент представляет собой рецепты различных наркотических средств, представленные в текстовом формате или в качестве последовательности слайдов.

4) пропаганда суицида. Согласно статье 110 УК РФ «Доведение до самоубийства» любые действия, направленные на пропаганду суицида должны подвергаться правовой оценке. В последнее время в социальных сетях стала популярным так называемая игра «синий кит» (и различные ее вариации), подстрекающая подростков на совершение действий, калечащих их психическое и физическое здоровье. Каждой жертве, вступившей в игру, назначался куратор, который через социальные сети отдавал ей «приказы». Итогом всей игры должна была быть смерть жертвы.

5) оправдание и популяризация терроризма. Доктрина информационной безопасности Российской Федерации обращает внимание на использование информационного воздействия на индивидуальное, групповое и общественное сознание террористическими организациями с целю вербовки в свои ряды, либо с целью подстрекания к совершению террористических актов.

6) подрыв суверенитета государства и политической стабильности. Данное деструктивное направление определяется пунктом 23 Доктрины информационной безопасности Российской Федерации, где выделяются следующие направления: подрыв суверенитета как государства в целом, так и его отдельных субъектов, подрыв политической и социальной стабильности.

7) отрицание традиционных ценностей. Согласно статье 5 Федерального закона «О защите детей от информации, причиняющей вред их здоровью и развитию» пропаганда нетрадиционных сексуальных отношений среди детей запрещена на территории РФ.

8) пропаганда сепаратизма. Данное деструктивное направление определяется статьей 280.1. УК РФ «Публичные призывы к осуществлению действий, направленных на нарушение территориальной целостности Российской Федерации», а также - пунктом 23 Доктрины информационной безопасности Российской Федерации, где пропаганда нарушения территориальной целостности РФ является одним из важнейших деструктивных направлений, которое требует пристального внимания и противодействия.

Таким образом, сформировано 8 признаков, по которым следует классифицировать деструктивный контент. Данное разграничение не является окончательной версией и может быть изменено, исходя из практической надобности исследования.

3 Методическое обеспечение для проведения риск-анализа контентов, циркулирующих в интернет-ресурсе

3.1 Качественный анализ угроз воздействия деструктивного контента

Прежде всего необходима классификация контентов, циркулирующих в интернет-ресурсе, а результаты такого анализа можно представить в виде древа (рис.3–4). В основе древа лежит угроза воздействия определенного типа деструктивного контента, после чего студентом определяются индуцированные ею риски.

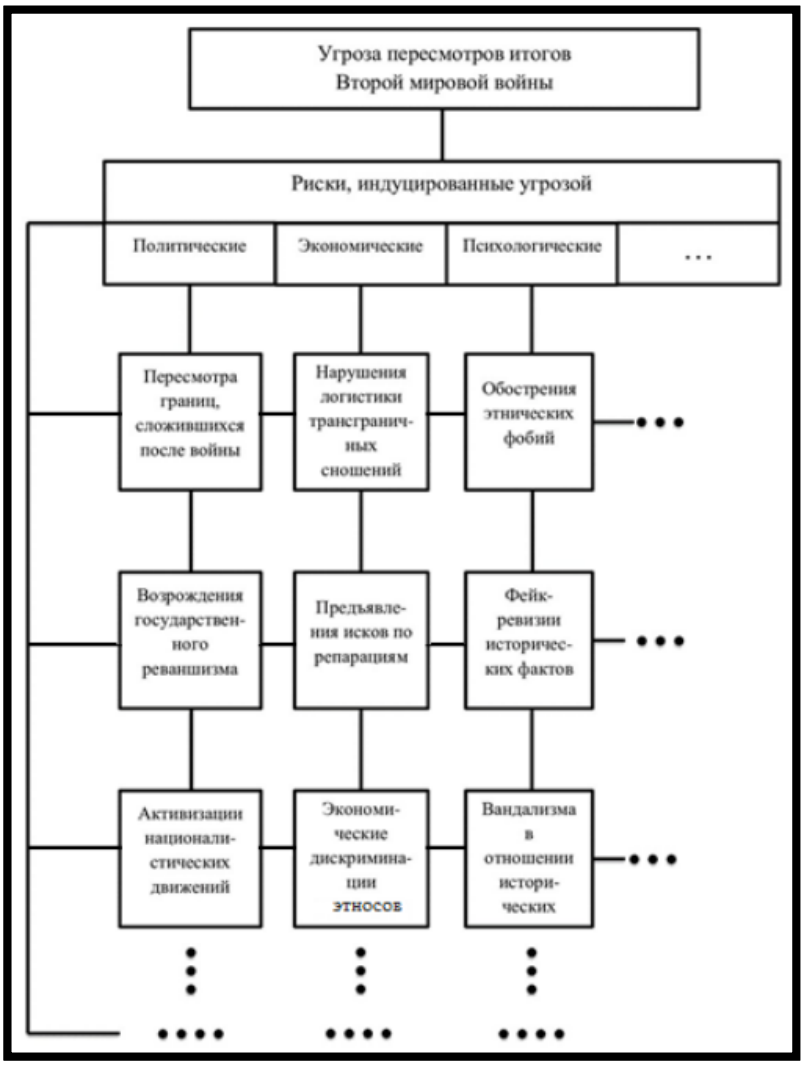

Рис. 3 Пример построения фрагмента дерева угроз и рисков

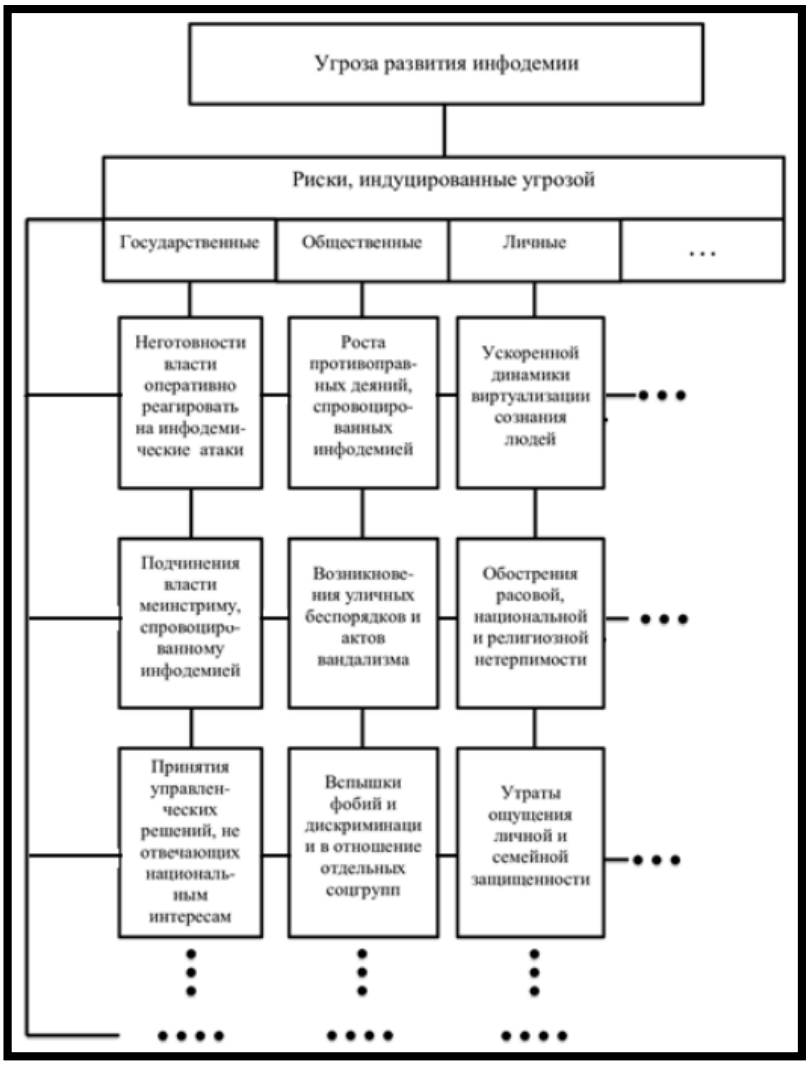

Рис. 4 Пример построения фрагмента дерева угроз и рисков

3.2 Параметры метрологии контентов

Объектом деструктивных воздействий на автоматизированные сети являются их пользователи. Если говорить о социальных автоматизированных сетях, то средством такого воздействия выступает распространяемая в них информация, побуждающая к опасным для социума действиям, которую зачастую называют деструктивным контентом (ДК). Вовлеченность пользователей в ДК, их реакция на его содержание и массовость этого явления определяют степень опасности информационно-психологической атаки [2].

Исходными выступают данные, находящиеся в открытом доступе, относительно просмотров, лайков, репостов и комментариев пользователей. Из этого представляется возможным определить соответствующие ареалы и, следовательно, вычислить ущербы, нанесенные социально-информационному пространству распространением ДК.

Для формулировки соответствующей методики введем следующие основные обозначения (табл. 2).

Таблица 2

Параметры, используемые для метрологии контентов

Обозначение параметра	Определение параметра
V	Множество пользователей ресурса
S	Множество просмотров контента
L	Множество лайков на контент
R	Множество репостов контента
G	Множество комментариев контента
∪	Операция объединения множеств
∩	Операция пересечения множеств
$\lvert . \rvert$	Операция определения мощности множества
A_{HI}	Ареал высокой вовлеченности
A_{MI}	Ареал средней вовлеченности
A_{LI}	Ареал низкой вовлеченности
$K_{S\|V}$	Заметность контента в исследуемом ресурса
$K_{L\|V}$	Востребованность контента в исследуемом ресурса
$K_{L\|S}$	Созвучность контента интересам пользователей исследуемого ресурса
$K_{R\|S}$	Тиражируемость контента пользователями исследуемого ресурса
$K_{G\|S}$	Комментируемость контента пользователями исследуемого ресурса
$K_{LRG\|S}$	Привлекательность контента для пользователей исследуемого ресурса
W_{HI}	Удельная мощность ареала высокой вовлеченности пользователей исследуемого ресурса
W_{MI}	Удельная мощность ареала средней вовлеченности пользователей исследуемого ресурса
W_{LI}	Удельная мощность ареала низкой вовлеченности пользователей исследуемого ресурса
$Risk_{HI}$	Риск невиртуальных деструктивных действий представителей A_{HI}
$Risk_{MI}$	Риск невиртуальных деструктивных действий представителей A_{MI}
$Risk_{LI}$	Риск невиртуальных деструктивных действий представителей A_{LI}

3.3 Базовые метрики контент-мониторинга

С точки зрения периода наблюдения возможны два подхода. Первый из них накопительный, когда от дискреты к дискрете мониторинга с помощью счетчиков, установленных в социальных сетях, суммируется количество лайков, репостов и комментариев, и мы получаем некоторую интегральную картину реакций пользователей на изучаемый контент. Второй подход носит дифференциальный характер, и учету подлежат только те реакции, которые последовали в период одного шага мониторинга. В этом случае во время жизни контента T0 можно наблюдать периоды роста T+ и спада T- популярности контента за счет сравнения (вычитания) показаний счетчиков реакций по соседним шагам. Получая таким образом скорость роста популярности контента, можно по аналогии найти ее ускорения путем сравнения дискрет. Такой параметр в период роста популярности дает возможность оперативно выявить наиболее востребованные пользователем контенты, а уже потом исследовать их тематические признаки и выделять среди них контенты, относящиеся к ДК [2].

По отношению к ДК можно выделить следующие ареалы пользователей:

а) низкой вовлеченности

$$A_{LI} = S\backslash(R \cup L \cup G); \quad (1)$$

б) средней вовлеченности

$$A_{MI} = (R \cup L \cup G)\backslash A_{HI}; \quad (2)$$

в) высокой вовлеченности

$$A_{HI} = R \cap L \cap G. \quad (3)$$

Удельный ущерб (нормированный по количеству пользователей) для ареалов можно представить в следующем виде:

а) низкой вовлеченности

$$\mathrm{W_{LI}} = \frac{|\mathrm{S}\backslash\mathrm{A_{LI}}|}{|\mathrm{V}|}; \quad (4)$$

б) средней вовлеченности

$$\mathrm{W_{MI}} = \frac{|\mathrm{A_{LI}}\backslash\mathrm{A_{HI}}|}{|\mathrm{V}|}; \quad (5)$$

в) высокой вовлеченности

$$\mathrm{W_{HI}} = \frac{|\mathrm{A_{HI}}|}{|\mathrm{V}|}. \quad (6)$$

Далее рассмотрим накопительный подход в мониторинге. Здесь важной характеристикой, очевидно, является восприимчивость контента пользователями сети (табл. 3), где интерес представляют доли его лайков |L|, репостов |R| и комментариев |G| по отношению к количеству |S| просмотров исследуемого контента. Чем выше эти доли, тем «заразительнее» был контент в сети. Следует заметит, что общее количество пользователей |V| в этом

параметре не участвует, ибо нас интересует лишь вирусность самого контента, а не пространства его диффузии.

Таблица 3

Метрики восприимчивости пользователями контента

Наименование метрик	Аналитические выражения метрик
Созвучность контента	$K_{L\|S} = \frac{\|L\|}{\|S\|}$
Тиражируемость контента	$K_{R\|S} = \frac{\|R\|}{\|S\|}$
Комментируемость контента	$K_{G\|S} = \frac{\|G\|}{\|S\|}$
Привлекательность контента	$K_{LRG\|S} = \frac{\|L \cup R \cup G\|}{\|S\|}$

Вторичную реакцию пользователей иллюстрирует таблица 4. Здесь рассматриваются ареалы реакций по отношению ко всему множеству пользователей исследуемого ресурса. Пояснить сущность вычисляемых параметров удобнее с помощью рисунка 4, где степень вовлеченности пользователей в содержание контента показана различными тонами (высокая – черным; средняя – темно-серым; низкая – светло-серым). Таблица 5 иллюстрирует эти множества аналитически через удельные оценки (относительно |V|) мощностей ареалов вовлеченности.

Таблица 4

Метрики первичной реакции пользователей ресурса на контент

Наименование метрик	Аналитические выражения метрик
Заметность контента в ресурсе	$K_{S\|V} = \frac{\|S\|}{\|V\|}$
Востребованность контента в ресурсе	$K_{L\|V} = \frac{\|L\|}{\|V\|}$

Таблица 5

Метрики вторичной реакции пользователей ресурса на контент

Наименование метрик	Аналитические выражения метрик
Удельная мощность ареала высокой вовлеченности пользователей ресурса в содержание контента	$W_{HI} = \frac{\|L \cap R \cap G\|}{\|V\|}$
Удельная мощность ареала средней вовлеченности пользователей ресурса в содержание контента	$W_{MI} = \frac{\|(L \cup R \cup G) \setminus (L \cap R \cap G)\|}{\|V\|}$
Удельная мощность ареала низкой вовлеченности пользователей ресурса в содержание контента	$W_{LI} = \frac{\|S \setminus (L \cup R \cup G)}{\|V\|}$

3.4 Оценка рисков

Обозначим вероятности реализации невиртуальных деструктивных действий для ареалов (рис. 5) пользователей следующим образом:

а) низкой вовлеченности P_{LI};

б) средней вовлеченности P_{MI};

в) высокой вовлеченности P_{HI}.

Зачастую вероятности устанавливаются экспертным путем и зависят от вирусности контента и менталитета ареала. Чем выше совпадение ДК и устремлений пользователей, тем больше значения этих вероятностей. Чаще всего имеет место соотношение:

$P_{HI} > P_{MI} > P_{LI}$.

Риск вовлеченности пользователей ресурса в невиртуальную деструктивную деятельность (как для взаимоисключающих ареалов) будет равен:

$$\mathrm{RiskI(t)} = \mathrm{W_{LI}(t)P_{LI}(t)} + \mathrm{W_{MI}(t)P_{MI}(t)} + \mathrm{W_{HI}(t)P_{HI}(t)}. \quad (7)$$

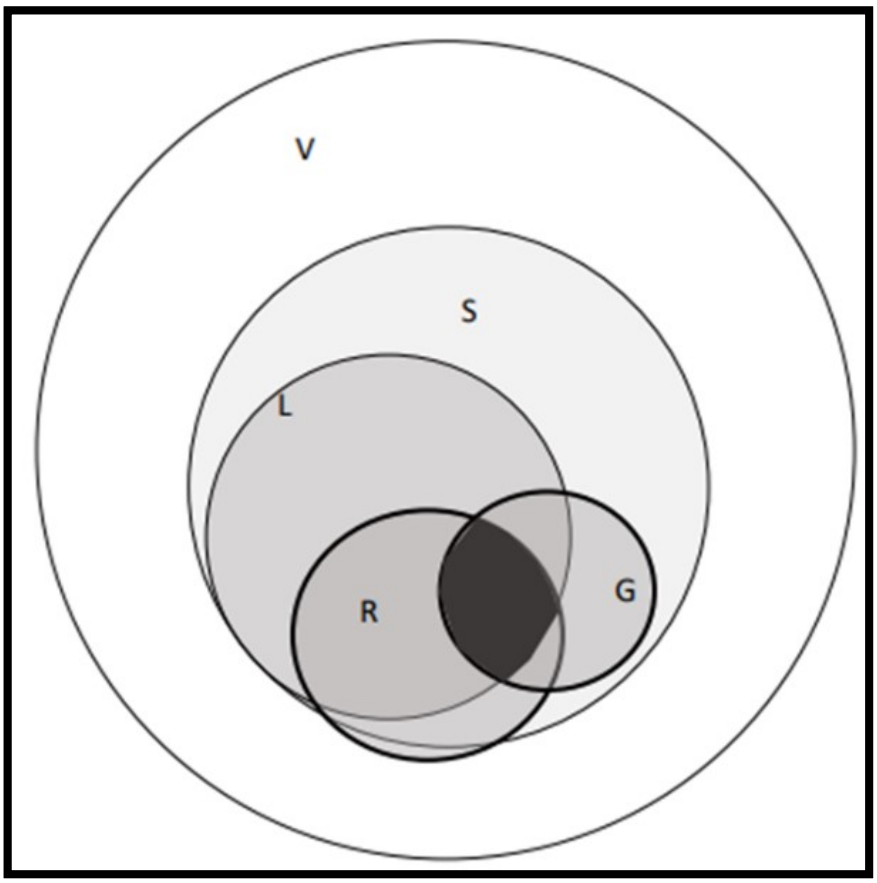

Рис. 5 Ареалы вовлеченности пользователей исследуемого ресурса

Таблица 6

Оценка рисков невиртуальных деструктивных действий пользователей, вовлеченных в содержание деструктивного контента

Наименование метрик	Аналитическое выражение метрик
Риск невиртуальных деструктивных действий представителей ареала высокой вовлеченности	$Risk_{HI} = W_{HI}P_{HI}$
Риск невиртуальных деструктивных действий представителей ареала средней вовлеченности	$Risk_{MI} = W_{MI}P_{MI}$
Суммарный риск по всем ареалам вовлеченности	$Risk_{HM} = Risk_{HI} + Risk_{MI}$
Риск невиртуальных деструктивных действий представителей ареала низкой вовлеченности	$Risk_{LI} = W_{LI}P_{LI}$
Суммарный риск по всем ареалам вовлеченности	$Risk_{HMl} = Risk_{HI} + Risk_{MI} + Risk_{LI}$

Последнее выражение (7) открывает широкий простор для многовариантного анализа и последующей оптимизации. Здесь параметры ущерба W_{LI}, W_{MI} и W_{HI} вычисляются в ходе мониторинга процесса распространения ДК.

Доли разнообразно реагирующих пользователей по отношению к общей мощности ресурса и сети позволяют оценить ожидаемую частоту невиртуальных деструктивных действий. Далее с помощью выражения (7) можно построить риск-модель исследуемого информационного пространства. Следует обратить внимание на временную зависимость параметров в модели (7). Это говорит о том, что необходима их регулярная актуализация как в ходе распространения контента, так и в динамике развития предпочтений и устремлений пользователей ресурсов (на основе систематических анонимных опросов, которые можно проводить в электронном виде).

4 Меры противодействия распространению деструктивного контента

Противодействие негативным информационно-психологическим воздействиям имеет громадное значение как для отдельного индивидуума, так и для общества в целом. Способы и механизмы противодействия основаны на тех же факторах и особенностях человеческого сознания, что и способы, и механизмы воздействия (реализуется одно массовое информационно-психологическое воздействие с целью противодействия другому) [4].

Противодействие угрозам нарушения информационно-психологической безопасности бывает техническое и организационно-правовое. Первое является совокупностью приемов, способов и средств воздействия, применяемых при информационно-психологическом противоборстве, а второе выражается в соответствующих нормативных актах и законах, принимаемых органами государственной и муниципальной власти.

Целью противодействия является нейтрализация деструктивного информационно–психологического воздействия (недопущение деморализации людей и т.п.) и последующее повышение в пользу социума соотношения морально– психологической устойчивости людей, поддержание ее на уровне, необходимом для успешного ведения социально-экономической деятельности социума.

Для достижения поставленной цели необходимо решить следующие задачи [4]:

– анализ морально–психологической обстановки в социуме;

– сбор, анализ и обобщение данных о возможностях осуществлять деструктивное информационно–психологическое воздействие на население социума;

– анализ содержания материалов СМИ, прогнозирование вероятного характера и возможных последствий осуществляемых деструктивных операций информационно–психологического воздействия;

– участие в определении основных задач и планировании мероприятий с учетом особенностей информационно-психологических воздействий;

– участие в проведении мероприятий по ослаблению деструктивного информационно–психологического воздействия;

– недопущение распространения дезинформации, проявления паники, растерянности среди населения;

– организация взаимодействия с возможными союзниками в интересах совместной реализации информационно–психологического противоборства.

Мероприятия по нейтрализации информационно-психологического воздействия предполагают (рис. 6):

– прогнозирование;

– профилактику;

– срыв (ослабление) информационно–психологического воздействия на население;

– ликвидацию последствий негативного информационно–психологического воздействия.

Прогнозирование предполагает выявление угроз и оценку ущерба применения средств деструктивного психологического воздействия. Прежде всего, необходимо выявить силы психологического воздействия, которые могут быть привлечены для массового деструктивного информационно–психологических воздействия, спрогнозировать направленность и результат их действия.

Профилактика информационно–психологического воздействия предполагает осуществление ряда превентивных мероприятий по снижению восприимчивости и подверженности населения информационно–психологическому воздействию. Основным инструментом здесь является систематическая контрпропаганда, разъяснение населению истинных целей, способов, возможных последствий акций информационно- психологического характера.

Срыв (ослабление) информационно–психологического воздействия достигается своевременным выявлением и дезактивацией сил и средств психологического воздействия (уничтожение пропагандистских материалов, пресечением слухов, панических настроений и т.п.).

Ликвидация последствий предполагает анализ и оценку результатов, наиболее слабых мест в системе информационно–психологической защиты, проведение психореабилитационных мероприятий и реализацию мер по оптимизации всей системы противодействия.

Рис. 6 Классификация мероприятий по нейтрализации информационно-психологического воздействия

ЗАКЛЮЧЕНИЕ

Направленность предлагаемого курсового проектирования во многом обусловлена внедрением Воронежским государственным техническим университетом стратегического проекта "Безопасный Интернет", инициированного Департаментом образования и науки Воронежской области. В этом случае студенты приобретают весьма актуальные компетенции в области обеспечения ИБ региона, а образовательный процесс имеет очевидную практическую направленность, которая простирается от курсовой работы до дипломного проектирования. Исходя из этого, в дальнейшем могут быть организованы мероприятия по профилактике в студенческой среде проявлений идеологии терроризма и экстремизма, а также выявление лиц с девиантным поведением, подверженных молодежным деструктивным субкультурам.

К продуктам проектирования следует отнести формирование и обновление базы данных контентов и интернет-ресурсов с признаками вышеуказанной деструктивности. Научно-методический интерес здесь представляет возможность организации интерактивного проектирования курса, когда на основе заданной базы данных и соответствующего разграничения доступа к ней для студентов обеспечивается автоматизированный процесс обучения, интегрированный в повестку дня информационного противостояния в интернет-пространстве [4], включая противоборство с бендеровской пропагандой в ходе реализации Специальной военной операции Вооруженных сил Российской Федерации на Украине.

СПИСОК ЛИТЕРАТУРЫ

1. 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);

2. 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);

3. 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);

4. 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);

5. Остапенко, А.Г. Краткие научно-методические рекомендации по формированию и выполнению технических заданий в области обеспечения информационной безопасности [Текст]/А.Г. Остапенко, М.Е. Волкова, Д.А. Нархов, А.А. Остапенко, А.В. Заряев, Т.Ю. Мирошниченко, П.Д. Федоров//Информация и безопасность. – 2020. – Т.23, №4, - С. 551-560;

6. К.А. Разинкин. Специалитет «Информационная безопасность»: краткие научно-методические рекомендации по выполнению курсового задания для дисциплины «введение в специальность» [Текст]/ К.А. Разинкин, В.Н. Кострова, В.М. Питолин, Н.М. Лантюхов, Д.А. Нархов / Информация и безопасность. – 2022. – Т.25, №1, - С. 155-158;

ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

к выполнению курсовой работы
для студентов специальностей
10.05.01 «Компьютерная безопасность»
10.05.02 «Информационная безопасность телекоммуникационных систем»
10.05.03 «Информационная безопасность автоматизированных систем»
очной формы обучения

Составители:
Остапенко Александр Григорьевич
Нархов Дмитрий Андреевич
Лантюхов Никита Михайлович
Егоров Анатолий Юрьевич
Остапенко Александр Алексеевич

Имеется в авторской редакции

Компьютерный набор Д.А. Нархова

Подписано к изданию
Уч.-изд . л. 1,5

ФГБОУ ВО «Воронежский государственный технический университет»
394006 Воронеж, ул. 20-летия Октября, 84