DOI 10.36622/VSTU.2022.25.1.013
УДК 004.056

СПЕЦИАЛИТЕТ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»: КРАТКИЕ НАУЧНО-МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ВЫПОЛНЕНИЮ КУРСОВОГО ЗАДАНИЯ ДЛЯ ДИСЦИПЛИНЫ «ВВЕДЕНИЕ В СПЕЦИАЛЬНОСТЬ»

К.А. Разинкин, В.Н. Кострова, В.М. Питолин, Н.М. Лантюхов, Д.А. Нархов

Рассматриваются научно-методические рекомендации, полезные для первокурсников в рамках выполнения ими индивидуальных курсовых заданий по дисциплине «Введение в специальность». Считая исключительно полезным освоение студентами методологии риск-мониторинга популярных интернет-ресурсов, авторы предлагают подходы к постановке соответствующих задач, способов их решения и структуризации курсовой работы. Ориентация на актуальные программные средства открывает перспективы для каждого первокурсника и выпускающей кафедры в целом получения емких, актуальных и научно-технически значимых результатов о социо-информационных рисках, порождаемых в интернет-ресурсах при распространении и восприятии контентов с признаками деструктивности. Работа ориентирована на специальности группы «Информационная безопасность». Предложения, сформулированные в ней, учитывают опыт подготовки и защиты курсовых работ 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 студентов направления «Информационная безопасность».

Ключевые слова: контент, риск, угрозы, аналитическая оценка, объект и предмет исследования, противоречия, результаты.

Введение

Студента, поступившего на специалитет «Информационная безопасность», одной из первых встречает дисциплина «Введение в специальность», изучение которой предполагает, прежде всего, его знакомство с пространством будущей профессии, а также привитие обретающему статус специалиста первичных базовых знаний и умений в области анализа безопасности информационных сетей и систем [1-4]. При этом дисциплина ориентирована на:

- освоение научно-методических основ кибербезопасности [1, 2], вовлечение будущих специалистов в проблематику сетевых войн [1, 3, 4] и защиты современного (мультисетевого) пространства [2-4];

-адекватное восприятие студентами сущности и важности проблемы обеспечения информационной безопасности (ИБ) через изучение основ и эффектов коммуникативного воздействия на психику индивида и социальной группы [3, 4], включая привитие информационного иммунитета и снижение рисков вовлечения студенческой молодежи в деструктивные сообщества;

- через ознакомление с цифровыми технологиями и методами социальной инженерии, демонстрация преимуществ отечественных демократических и духовно-нравственных ценностей и традиций, тем самым снижая риски участия студенческой молодежи в операциях кибер-преступных группировок и противоправных акциях (цветных революциях) протеста [3, 4].

Неслучайно курсовая работа дисциплины «Введение в специальность» посвящена риск-мониторингу интернет-ресурсов, оказывающих наиболее существенное влияние на общественное сознание и ИБ молодежной интернет-аудитории [1, 2].

Теоретические положения

В рамках курсового проектирования студентам предлагается провести самостоятельную исследовательскую работу,

которая содержит результаты теоретических и практических исследований, например, анализа результатов с помощью программного комплекса Netepidemic, в результате которого будущие специалисты приобретают навыки работы с научной и методической литературой, а также со специализированными программными комплексами.

При этом контексте наших специальностей мы должны «танцевать от печки», т. е. от угроз объекту исследования и через оценку рисков их реализации обязаны дойти до риск-управления в интересах обеспечения ИБ личности, общества и государства через приобретение студентами следующих профессиональных компетенций:

– знает понятия социальной системы и её разновидностей, информационно-психологического воздействия и управления в многообразии их видов, объектов, эффектов, способов, средств и приёмов, место и роль технологии массовых коммуникаций и пропаганды в проблеме обеспечения ИБ;

– умеет классифицировать контенты и социальные сети как среды их распространения в условиях информационного противоборства, оценивать риски вовлеченности пользователей в деструктивные контенты и онлайн-сообщества, включая их мониторинг в интернет-пространстве.

Задачи работы представляют собой последовательность действий:

- сбор статистики для анализа публичной страницы/группы/канала;

- составление структуры рассматриваемого ресурса и его структурно-функциональной схемы;

- построение моделей и классификация деструктивных контентов;

- изучение возможных угроз от контент-воздействия;

- выявление и классификация реакций пользователя исследуемого ресурса;

- мониторинг контентов в социальной сети с помощью программного комплекса «Netepidemic-CMSN»;

- составление портрета регионального пользователя данной публичной страницы/группы/канала;

- выработка рекомендаций в целях противодействия деструктивному контент-влиянию.

Методическое обеспечение

Конечной целью работы является риск-анализ процессов распространения и восприятия контентов с признаками деструктивности в региональных интернет-сообществах, что является угрозой нарушения информационно-психологической безопасности особенно в молодежной среде, активно пользующейся социальными сетями. Выявление таких контентов в заданных пабликах позволяет в дальнейшем оценить вовлеченность аудитории в их содержание через подсчет количества просмотров, лайков и репостов в период жизни исследуемого контента. При этом степень опасности (риск) выявленного поста деструктивного содержания может быть охарактеризована отношением количества просмотров, лайков, репостов и комментариев к общему количеству зарегистрированных в сообществе пользователей на каждом конкретном дискретном шаге процесса наблюдения. Рассматривая все множество зарегистрированных контентов с признаками деструктивности, выявленных в заданном сообществе, можно оценить его риск-параметры в отношении постов определенной тематической направленности (тематическое моделирование).

С использованием вышеуказанных данных фактически представляется возможность оценить ареалы распространения и восприятия деструктивов, выявленных в региональном социо-информационном пространстве. В этой ситуации студент получает навыки риск-мониторинга заданного объекта (регионального интернет-сообщества) в ходе курсового проектирования. Анализ

результатов мониторинга позволяет проектанту также выработать практические рекомендации по информационному противодействию потокам деструктивных контентов (фейков), которые существенно выросли в современных геополитических условиях.

Заключение

Ориентация предлагаемого курсового проектирования во многом обусловлена реализацией Воронежским государственным техническим университетом стратегического проекта «Безопасный интернет», инициированного Департаментом образования и науки Воронежской области. В этом случае студенты приобретают весьма актуальные компетенции в сфере обеспечения ИБ региона и учебный процесс имеет очевидную практическую направленность, которая просматривается от курсового до дипломного проектирования специалитета «Информационная безопасность». На этой основе в перспективе может быть организована деятельность по активизации профилактики проявлений в студенческой среде идеологии терроризма и экстремизма, и выявления лиц с девиантным поведением, подверженных воздействию молодежных деструктивных субкультур.

К продуктам проектирования прежде всего следует отнести формирование и актуализацию базы контентов и интернет-ресурсов с признаками вышеупомянутой деструктивности. Научно-методический интерес здесь представляет возможность организации интерактивного курсового проектирования, когда на основе данной базы данных и соответствующего разграничения доступа к ней студентов обеспечивается автоматизированный учебный процесс, интегрированный в насущную проблематику регионального информационного противоборства в интернет-пространства. Таковой видится перспектива развития настоящего проекта.

Список литературы

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

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

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

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

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

Поступила в редакцию 20.02.2022

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

Лантюхов Никита Михайлович– студент, Воронежский государственный технический университет, e-mail: mnac@comch.ru

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

SPECIALTY "INFORMATION SECURITY": BRIEF SCIENTIFIC AND METHODOLOGICAL RECOMMENDATIONS FOR THE IMPLEMENTATION OF THE COURSE ASSIGNMENT FOR THE DISCIPLINE "INTRODUCTION TO THE SPECIALTY"

K.A. Razinkin, V.N. Kostrova, V.M. Pitolin, N.M. Lantyukhov, D.A. Narhov

Scientific and methodological recommendations useful for first-year students in the framework of their individual course assignments in the discipline "Introduction to the specialty" are considered. Considering it extremely useful for students to master the methodology of risk monitoring of popular Internet resources, the authors propose approaches to setting appropriate tasks, ways to solve them and structuring course work. Orientation to current software tools opens up prospects for each freshman and the graduating department as a whole to obtain capacious, relevant and scientifically and technically significant results on socio-informational risks generated in Internet resources when distributing and perceiving content with signs of destructiveness. The work is focused on the specialties of the Information Security group. The proposals formulated in it take into account the experience of preparing and defending term papers in the above-mentioned specialties that 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 students of the direction "Information Security".

Keywords: content, risk, threats, analytical assessment, object and subject of research, contradictions, results.

Submitted 20.02.2022

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

Nikita M. Lantyukhov – Student, Voronezh State Technical University, e-mail: mnac@comch.ru

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