УДК 364.2

МОДЕЛЬ МЕР ПРОТИВОДЕЙСТВИЯ ДЕСТРУКТИВНОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ

Маматов М.Р., Бурхонов Т.У.[1]
[1]Самаркандский филиал Ташкентского университета информационных технологий имени Мухаммада ал-Хорезми, Самарканд, Узбекистан

Аннотация. *В данной статье разработаны модели мер противодействия деструктивной информации в сети Интернет. В статье рассматриваются различные меры противодействия деструктивной информации и выделяются их виды. Определяется классификация мер противодействия по различным признакам, в том числе, по виду информации, против которой направлены меры, по каналу распространения информации, по целевой аудитории данной информации, по оперативности и способу противодействия. Также определяется набор метрик, характеризующих меры противодействия. С учетом выделенных классов и их признаков, то есть качественных характеристик мер противодействия, а также выделенных метрик, то есть количественных характеристик мер, формируется их модель. В работе также описано применение данной модели в общем процессе противодействия деструктивной информации.*

Ключевые слова: *Деструктивная информация, меры противодействия, модель, сеть Интернет.*

I. ВВЕДЕНИЕ

В последнее время все актуальнее становится проблема материального и информационно-психологического ущерба от деструктивной информации, то есть информации, представляющей угрозу для сознания, духовной жизни и информационной деятельности гражданина, и общества в целом. В рамках разработки методики противодействия такой информации в статье предлагается модель мер противодействия деструктивной информации в сети Интернет.

II. ОСНОВНАЯ ЧАСТЬ

Для защиты от деструктивной информации применимы следующие способы: управление, препятствие, регламентация, принуждение и побуждение. Управление охватывает и описывает применение всех остальных способов (препятствие, регламентация, принуждение и побуждение). Для описания видов, способов распространения и противодействия деструктивной информации используются способы регламентации и принуждения. Средствами, реализующими данные способы, являются акты, принятые в различных организациях и определенные на основе законов Республики Узбекистан. Методы защиты от деструктивной информации на самом верхнем уровне можно разделить на технические *(соответствуют физическим, аппаратным, программным средствам защиты)*, такие как блокировка источников деструктивной информации, и организационные *(соответствуют организационным, законодательным, морально-этичес-*

ким средствам защиты), такие как информирование пользователей. В настоящее время существует несколько механизмов защиты от деструктивной информации [1]. К ним относится:

1) ручная классификация информационной продукции по категориям доступа к просмотру, при этом механизм защиты предполагает выдачу предупреждения о категории доступа;

2) ручная блокировка ресурсов, содержащих нежелательную информацию, с использованием реестра блокировок;

3) автоматизированные системы защиты от информации в виде отдельных опций в операционной системе (ОС). Ограничение доступа к деструктивной информации, определенное законами РУз, осуществляется методами препятствия, и зависит от способа распространения деструктивной информации. Методы препятствия подразумевают автоматизированное применение программных и аппаратных средств, ограничивающих доступ к деструктивной информации. В настоящее время основными способам препятствия распространению деструктивной информации является блокировка соответствующих ресурсов [2], а также системы родительского контроля. Кроме способов препятствия для ограничения доступа к деструктивной информации также применим способ побуждения. В данном случае используются морально-этические средства, в том числе побуждающие родителей не допускать детей к веб-сайтам, содержащим деструктивную и нежелательную информацию. Также необходимо повышать информированность населения об ущербе от распространения такой информации, наказании за ее распространение и средствах защиты.

В таблице 1 конкретные средства защиты от информации разделены на классы. Эти классы могут пересекаться. Класс методов защиты от деструктивной информации зависит от их вида, способа и скорости ее распространения *(в частности, информация может выкладываться на сайтах или вбрасываться для последующего лавинного распространения)*, целевой аудитории, влияния средств защиты на права граждан.

Класс способа защиты от информации, как и класс средств защиты от информации, являются параметрами предлагаемой модели мер противодействия. Разработанная модель описывается следующими параметрами: класс способа защиты от информации; класс средства защиты от информации; вид информации *(деструктивная, нежелательная, вредоносная, сомнительная)*; тип информационного объекта *(сообщение, рисунок)*; канал распространения информации *(новости, социальные сети, веб-сайты)*; целевая аудитория *(дети, взрослые)*; влияние на модель распространения информации *(поскольку модель распространения информации в общем подходе представляется в виде графа, влияние может заключаться в удалении связей/узлов графа, либо изменении значений метрик для узлов/связей)*; метрики *(эффективность меры, побочный ущерб при реализации меры, стоимость меры, степень ущерба от нежелательной информации)*. Данные параметры являются основой для выбора меры противодействия и позволяют сопоставить модель меры

противодействия и другие модели в рамках общей методики защиты от информации *(такие как модель распространения информации, модель источника деструктивной информации, модель объект воздействия информации и другие)*. В таблице 2 приведены примеры значений параметров мер противодействия разных классов.

Таблица 1. Соответствие между способами и средствами защиты от информации

Классы способов защиты от информации	**Классы средств защиты от информации**	**Средства защиты от информации**
препятствие (физическая защита)	физические, аппаратные и программные	фильтрация сообщений, блокировка источников деструктивной информации, автоматизированные системы защиты от информации в виде отдельных опций в ОС, системы родительского контроля
маскировка (шифрование данных)	программные, аппаратные	блокировка источников деструктивной информации
регламентация (определение процедур манипуляции данными)	организационные, законодательные	акты, принятые в различных организациях и определенные на основе законов РУз
управление *(выделение основных компонентов информационной системы и управление ими)*	организационные, физические, программные и аппаратные	системы мониторинга деструктивной информации и выбора мер по противодействию
принуждение (введение средств защиты для выполнения регламента)	организационные, законодательные, программные, аппаратные, физические	фильтрация сообщений, блокировка источников деструктивной информации, автоматизированные системы защиты от информации в виде отдельных опций в ОС, системы родительского контроля
побуждение (использование Этических и личностных соображений для выполнения регламента)	морально-этические	информирование пользователей, предупреждение о категории доступа информации, побуждение родителей не допускать детей к веб-сайтам, содержащим деструктивную информацию, повышение информированности населения об ущербе от распространения нежелательной информации, наказании за ее распространение и средствах защиты

Общий подход противодействия деструктивной информации включает определение класса информации, определение класса мер противодействия и выбор оптимальных мер. Выбор класса мер осуществляется на основе класса информации, канала ее распространения, типа, и целевой аудитории (рис.1). Разным совокупностям классов данных объектов и субъектов ставятся в соответствие разные классы контрмер (табл. 2). Затем из выбранного класса (классов) выбираются оптимальные меры с учетом метрик, включенных в модель.

Таблица 2. Примеры значений параметров мер противодействия разных классов

Класс информационного объекта	**Канал распространения**	**Целевая аудитория**	**Класс способа защиты от информации**
Большие информационные объекты: информационная система, социальная сеть, мессенджер, микроблог, форум, игровой портал, медиа-портал, веб-сайт, и т. д.	Большие информационные объекты: информационная система, социальная сеть, мессенджер, микроблог, форум, игровой портал, медиа-портал, веб-сайт, и т. д.	Взрослые Дети	препятствие (физическая защита)
Средние информационные объекты: веб-страница, группа, публичная страница, канал, статья, страница форума, и т. д.	Большие информационные объекты: веб-сайт, социальная сеть, мессенджер	Взрослые Дети	маскировка (шифрование данных)
Малые информационные объекты: пост, сообщение, комментарий, заголовок, текст статьи, медиа-объект (изображение, аудио, видео), и т. д.	Большие информационные объекты: веб-сайт, социальная сеть, мессенджер	Взрослые Дети	регламентация (определение процедур манипуляции данными)

Рис.1. Концепция второго этапа подхода к противодействию

III. ЗАКЛЮЧЕНИЕ

Таким образом, в статье описана модель мер противодействия и принцип ее применения в общем подходе противодействия деструктивной информации. В дальнейшей работе предполагается формализовать модель, разработать конкретные методики выбора мер противодействия в рамках предложенного подхода и провести эксперименты по оценке эффективности подхода.

ЛИТЕРАТУРА

[1] *Тумбинская М. В.* Системный подход к обеспечению защиты от нежелательной информации в социальных сетях // Вопросы кибербезопасности. 2017. № 2 (20). С. 30–44.

[2] *Котенко И. В., Саенко И. Б., Чечулин А. А.* Защита от нежелательной и вредоносной информации в глобальных информационных сетях // Информационно-психологическая

и когнитивная безопасность: состояние и задачи: коллективная монография / Под ред. И. Ф. Кефели, Р. М. Юсупова. СПб.: Изд-во «Аврора», 2017. С. 207–229.

Поступила в редакцию 25.08.2022

Цитирование: *Маматов М.Р., Бурхонов Т.У.* Модель мер противодействия деструктивной информации в сети интернет // Международный журнал теоретических и прикладных вопросов цифровых технологий. – 2022. – №1(1). –С. 53-57.

MODEL OF MEASURES TO COUNTER THE DESTRUCTIVE INFORMATION ON THE INTERNET

Mamatov M.R., Burkhonov T.U.[1]
[1] Samarkand branch of Tashkent University of information technologies named after Muhammad al-Khwarizmi, Samarkand, Uzbekistan

Abstract. *The work discusses various measures to counteract destructive information and highlights their types. The classification of countermeasures is determined according to various criteria, including the type of information against which the measures are directed, the channel for disseminating information, the target audience of this information, the efficiency and method of counteraction. A set of metrics characterizing countermeasures is also determined. Taking into account the distinguished classes and their characteristics, that is, the qualitative characteristics of countermeasures, as well as the distinguished metrics, that is, the quantitative characteristics of measures, their model is formed. The paper also describes the application of this model in the general process of counteracting destructive information.*

Keywords: *Destructive information, countermeasures, model, Internet.*