ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Региональный учебно-научный центр по проблемам информационной безопасности

Кафедра систем информационной безопасности

«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». - В.В. Путин, заседание Совета Безопасности РФ, 26.10.17.

Инвест-релиз проекта «БЕЗОПАСНЫЙ ИНТЕРНЕТ»

Руководитель проекта:
Руководитель Регионального учебно-научного центра по проблемам информационной безопасности (РУНЦ), заведующий кафедрой систем информационной безопасности
Остапенко Александр Григорьевич

HTTP:
безопасный-интернет.рф
kafedrasib.ru
E-mail:
mnac@comch.ru
sub316@mail.ru

Воронеж
2018

1. Тема.

Безопасный Интернет.

1.1. Приоритет стратегии.

Обеспечение Интернет-безопасности региональных кластеров социальных сетей за счет снижения рисков распространения в них деструктивного контента.

1.2. Категория проекта: Поддержка импортозамещающих научных и научно-технических проектов высокой социальной значимости.

1.3. Наименование комплексной научно-технической программы и технологии/ технологического направления: Управление информационными рисками и обеспечение безопасности электронных технологий.

1.4. Научно-технологическая задача / технологический барьер от Индустриального партнера, на решение которых направлены ожидаемые результаты проекта: Автоматизация мониторинга социальных сетей с целью выявления и анализа деструктивного контента в региональных пабликах.

2. Ключевые слова

2.1. На русском языке: деструктивный контент, социальные сети, паблики, распространение контента, социальные связи, мониторинг сетевой структуры и трафика, обнаружение деструктивного контента в социальной сети, определение параметров и характеристик деструктивного контента.

2.2. На английском языке: destructive content, social networking, public pages, content distribution, social connections, monitoring of network structure and traffic, destructive content detection in the social network, destructive content characteristics finding.

3. Цель (цели)

Повышение информационной защищенности Интернет-пользователей, проживающих на территории Воронежской области Российской Федерации, за счет автоматизированного выявления деструктивного контента в популярных в регионе пабликах и определения параметров (характеристик) его распространения, включая визуализацию результатов данного мониторинга для лиц, принимающих решение в условиях противоборства в социальных сетях.

В этом контексте объектом исследования выступают сообщества социальных сетей для общения, наиболее посещаемые региональными Интернет-пользователями.

4. Целесообразность проведения исследований

4.1. Описание проблемы

Коммуникация – есть важнейшее свойство живой природы. В ней особое место занимает человек, как единственный вид, способный говорить сквозь время (созвучно религиозным учениям о бессмертии души). Наскальная живопись, дошедшая до нас через тысячелетия, яркий пример того, как художественные символы выступают в качестве послания потомкам. Однако, качественный скачок произошел у людей позднее, с появлением языка и письменности (их трансляторами сквозь время выступала церковь). Именно тогда тексты стали первыми средствами вирусной коммуникации, способной заражать сознание людей новыми идеями. Неслучайно Киплинг считал слова самым сильным наркотиком, который изобрело

Человечество. Понятные и общепризнанные символы, образующие слова, обеспечили широкое распространение идей и доминирование на планете человека как вида живых существ. Границы человеческого общения революционно расширились с появлением гаджетов, порожденных симбиозом бинарного языка и цифровой электроники. Благодаря им мы сегодня имеем глобальную человеческую коммуникацию, в основе которой лежит словесная конструкция – контент, создающий новую реальность. Видимо, именно поэтому возник соблазн контролировать ее, основанный на чрезвычайном любопытстве человека и его значительной зависимости от содержания получаемых контентов. Однако главное достоинство коммуникации лежит не в возможности контролировать реальность, а в способности обрести человеческому виду вечность (за счет генерации и передачи потомкам инновационных знаний и культурно-нравственных ценностей, снижающих риски реализации надвигающихся вызовов и гарантирующих сохранение и развитие вида).

В этом контексте злоумышленниками следует считать создателей контента, побуждающего личность к деструктивным действиям. Такой (деструктивный) контент оказывает разрушающее воздействие на человека, а глобальная коммуникация открывает злоумышленникам заманчивые перспективы управления массовым сознанием. Отсюда борьба с распространением деструктивного контента приобретает особую значимость в настоящее время, так как он сеет хаос и не должен формировать будущее. Благородство миссии специалистов в области информационной безопасности, прежде всего, видится именно в этом.

Глобальность обозначенной проблемы требует учета ее геополитической составляющей. И дело здесь в том, что действующая стратегия национальной безопасности США, как лидера западной цивилизации, не оставляет надежд на миролюбивую внешнюю американскую политику в отношении России. С другой стороны, привлекательность для Запада российских природных ресурсов и затруднительность их захвата в результате военной агрессии перемещает противоборство в информационное пространство с надеждой для западных глобалистов развалить РФ через атаки ее граждан деструктивным контентом, девальвирующим культурные ценности и традиции, нацеленным на нравственную деградацию и духовное обнищание населения, порождающим национальную и религиозную рознь в обществе. Как следствие, ареной этого ожесточенного противоборства сейчас стали столь популярные социальные сети.

4.2. Обоснование актуальности

Сила и риски России, вытекающие из ее многонациональности и культурного разнообразия, диктуют в ходе вышеупомянутого информационного противоборства необходимость учета регионального аспекта. Природные, этнические и религиозные различия субъектов РФ исторически сформировали весьма пеструю ментальность ее регионов, которая, несомненно, отразилась и на их пользователях Интернет-пространства. Информационная модель такого пользователя может существенно розниться для территорий Российской Федерации (свыше 100 народностей, 11 часовых поясов и 8 климатических зон). Очевидным тому свидетельством следует считать региональные паблики. Десятки таких Интернет-сообществ функционируют в каждом регионе России, где жители обсуждают темы, насущные для

своей территории. Всё это перемещает «битву контентов» в республики, края и области РФ. Федеральные обобщения в данном случае будут напоминать поиск «средней температуры по больнице». Поэтому именно модель регионального Интернет-пользователя (РИП), отражающая его коммуникационные предпочтения в социальных сетях и сообществах, должна лежать в основе этой битвы, включая процедуры выявления деструктивных контентов, измерения их параметров и оценки ареала распространения, оперативное противодействие. Уместно здесь отметить тот факт, что практикуемое при противоборстве блокирование источников деструктивных контентов и даже целых Интернет-сервисов (Китай) малоэффективно в долгосрочной перспективе.

Напротив, сейчас остро необходим инструментарий, который оперативно (по возможности, в реальном масштабе времени) будет реагировать на контент-атаки. В виду обилия и изощренности последних, осуществлять вышеизложенное только в ручном режиме далее не представляется возможным. Теперь эту процедуру придется в автоматизировать, программным путем идентифицируя вредоносы и оценивая их опасность в региональном Интернет-пространстве. При этом исключительно организационно-правовое реагирование дает значительное отставание в информационной борьбе. В этом контексте цензура через модерацию социальных сетей имеет явно выраженные недостатки человеческого фактора: субъективизм суждений и оценок, ограниченность быстродействия обработки данных и принятиия решения в случае лавинообразного вброса деструктивного контента. Здесь нужна оперативная контр-пропаганда в Интернет-сообществах (телевидения, которое мало смотрит молодежь, тут явно недостаточно), опирающаяся на предлагаемый программный инструмент и модель РИП, в каждом субъекте РФ.

4.3. Новизна и научно-технический уровень

1. Опора программно-технического комплекса (ПТК) на модель регионального Интернет-пользователя, сформированную с помощью социологических опросов пользователей в конкретном субъекте РФ.

2. Ориентация ПТК на деструктивные признаки контента (сепаратизм, экстремизм, терроризм и др.) с целью его выявления и определения ареала распространения в региональном Интернет-пространстве.

3. Реализация в ПТК внешнего (без интеграции с помощью административного ресурса дополнительных инструментов веб-аналитики в отдельных соцсетях) мониторинга процессов распространения деструктивного контента в Интернет-сообществах, пользующихся популярностью в рассматриваемом регионе.

4. Применение современных моделей процессов, протекающих в информационных социальных сетях, а также технологий машинного обучения и BigData для определения региональной специфики и уточнения модели РИП отражает научно-технический уровень проекта.

5. Задачи и возможные пути их решения

Для достижения поставленной цели необходимо решение следующих задач:

1. Итерационная актуализация автоматизированной модели регионального Интернет-пользователя и систематическое обновление РРДК.

2. Создание компонента ПТК для сканирования региональных пабликов.
3. Создание компонента ПТК для выявления деструктивного контента.
4. Создание компонента ПТК для определения метрик и прогнозировнаия ареала распространения деструктивного контента.
5. Создание личного кабинета оператора ПТК.

При этом просматриваются следующие пути их решения:

1. Формирование методического обеспечения на основе оригинальных разработок кафедры (п.7.1) в области риск-анализа деструктивных информационных воздействий.
2. Разработка алгоритмического и программного обеспечения ПТК на основе технологий BigData и машинного обучения.
3. Итерационное повторение анонимного анкетирования в пабликах для уточнения и расширения автоматизированной модели регионального Интернет-пользователя, включая анализ модели для получения выборки вероятных распространителей и потребителей деструктивного контента.

6. Ожидаемые результаты

6.1. Описание результатов исследований

В результате реализации проекта должны быть обеспечены:

1. Сканирование (на предмет выявления деструктивных контентов) региональных пабликов, охватывающих (с учетом пересечений) абсолютное большинство аудитории региональных пабликов. Заказчик может задать конкретный перечень пабликов либо процент охвата аудитории.
2. Выявление в вышеуказанных пабликах контента с признаками деструктивности, определенными Концепцией национальной безопасности и Доктриной информационной безопасности Российской Федерации, Федеральными законами «Закон о средствах массовой информации» и «О защите детей от информации, причиняющей вред их здоровью и развитию», «Единым реестром запрещенной информации» Роскомнадзора РФ. Заказчик вправе задать отдельно интересующие его признаки деструктивности контента.
3. Визуализация выявленного контента, включая его параметры на мониторе оператора проекта. Заказчик определяет максимально допустимый период выявления деструктивного контента, например, в пересчете на один анализируемый паблик (при последовательном их обходе).
4. Определение следующих параметров деструктивного контента (в установленный выше период). К примеру:

- время и место появления;
- источник вброса;
- значение параметров риска вовлеченности пользователей;
- прогнозируемый период активности контента;
- прогнозируемый ареал распространения (на пике популярности) контента.

Перечень параметров может быть сокращен либо расширен заказчиком с соответствующей коррекцией допустимого периода выявления контента.

5. Исходя из ареала и анализа комментариев контента, оценка и визуализация риска деструктивных действий Интернет-пользователей региона под влияни-

ем распространяемого контента. Скорее всего, заказчика будет интересовать некий порог одобрения аудиторией выявленного и распространяемого деструктивного контента.

6. Отслеживание и визуализация вышеуказанных параметров (в течение всего прогнозируемого периода активности с регулярным обновлением) наиболее опасных контентов. Заказчик вправе задать периодичность наблюдения за таким контентом.
7. Актуализация (на основе периодически реализуемых паблик-опросов) модели регионального Интернет-пользователя, в том числе с учетом накапливаемого (по вышеуказанному регламенту) регионального реестра РРДК деструктивных контентов и реестра генерирующих их источников, включая аналитику о динамике параметров модели. Заказчик может задать периодичность обновления модели и ее анализа.

Примечание: Вышеизложенное имеет отношение исключительно к русскоязычным открытым Интернет-сообществам.

6.2. Значимость для реализации стратегических документов

Разработка ПТК соответствует приоритетам научно-технологического развития Российской Федерации, определенных Стратегией научно-технологического развития Российской Федерации в области противодействие техногенным, биогенным, социокультурным угрозам, терроризму и идеологическому экстремизму, киберугрозам и иным источникам опасности для общества, экономики и государства. Проект реализуется в соответствии с требованиями Стратегии национальной безопасности Российской Федерации (утверждена Указом Президента РФ от 31.12.15 № 683), Доктрины информационной безопасности Российской Федерации (утверждена Указом Президента РФ от 05.12.2016 № 646), стратегии развития информационного общества Российской Федерации (утверждена Указом Президента РФ от от.05.2017 № 203) и Программы «Цифровая экономика Российской Федерации» (утверждена распоряжением Председателя Правительства РФ от 28.07.2017 № 1632-р).

7. Научный (научно-технический) задел

7.1. Результаты исследований в предметной области проекта

1. Монографии:
   - 1.1. Социальные сети и деструктивный контент/ Остапенко А.Г., Паринов А.В., Калашников А.О. и др.; Под ред.чл.-корр. РАН Д.А. Новикова. – М.: Горячая линия – Телеком, 2017. – 276 с.: ил.
   - 1.2. Эпидемии в телекоммуникационных сетях/ Остапенко А.Г., Радько Н.М., Калашников А.О. и др.; Под ред.чл.-корр. РАН Д.А. Новикова. – М.: Горячая линия – Телеком, 2017. – 284 с.: ил.
   - 1.3. Атакуемые взвешенные сети/ Остапенко А.Г., Плотников Д.Г., Калашников А.О. и др.; Под ред.чл.-корр. РАН Д.А. Новикова. – М.: Горячая линия – Телеком, 2017. – 248 с.: ил.
2. Статьи в журналах, индексированных в базе SCOPUS:
   - 2.1. Ostapenko, A.G. Denial of service in components of information telecommunication systems through the example of “network storm” attacks / A.G.

Ostapenko, S.S. Kulikov, N.N. Tolstykh, Y.G. Pasternak, L.G. Popova // World Applied Sciences Journal. – 2013. – 25 (3). – P. 404-409.

2.2. Ostapenko, A.G. The usefulness and viability of systems: Assessment methodology taking into account possible damages / A.G. Ostapenko, E.F. Ivankin, V.S. Zarubin, A.V. Zaryaev // World Applied Sciences Journal. – 2013. – 25 (4). – P. 675-679.

2.3. Ostapenko, G.A. Analytical estimation of the component viability of distribution automated information data system / G.A. Ostapenko, D.G. Plotnicov, O.Y Makarov, N.M. Tikhomirov, V.G. Yurasov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 416-420.

2.4. Ostapenko, G.A. Analytical models of information-psychological impact of social information networks on users / G.A. Ostapenko, L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov, K.V. Simonov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 410-415.

2.5. Radko, N.M. Assessment of the system's EPI-resistance under conditions of information epidemic expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, D.V. Gusev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (3). – P. 1781-1784.

2.6. Radko, N.M. Peak risk assessing the process of information epidemics expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, A.S. Avdeev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 251-255.

2.7. Islamgulova, V.V. Discreet risk-models of the process of the development of virus epidemics in non-uniform networks / V.V. Islamgulova, A.G. Ostapenko,,N.M. Radko, R.K. Babadzhanov, O.A. Ostapenko // Journal of Theoretical and Applied Information Technology. – 2016. – Vol. 86. – No.2. – P. 306-315.

3. Свидетельство РОСПАТЕНТа о государственной регистрации программы для ЭВМ №2016662015. Netepidemic, от 09.01.17.

7.2. Материально-техническая база

Реализация проекта осуществляется с использованием материально-технической базы ВГТУ

7.3. Коллектив ключевых исполнителей

Руководитель проекта Остапенко Александр Григорьевич, руководитель Регионального учебно-научного центра по проблемам информационной безопасности, заведующий кафедрой систем информационной безопасности ВГТУ.

Структурные подразделения университета – участники проекта

Кафедра систем информационной безопасности ВГТУ.

Внешние участники проекта

Правительство Воронежской области (инициатор проекта) в лице его департамента образования, науки и молодежной политики, где в настоящее время проходит апробацию **стартовая версия** автоматизированной модели РИП, подготовленная исполнителями проекта.

7.4. Развитие научных заделов

1. Разрабатываемое обеспечение внедряется в учебный процесс вуза по специальностям 10.05.01 «Компьютерная безопасность», 10.05.02 «Информационная безопасность телекоммуникационных систем» и 10.05.03 «Информационная безопасность автоматизированных систем», обеспечивая тем самым его инновационную направленность и рост качества подготовки специалистов. В рамках учебного процесса (студенческая НИР) ежедневно обновляется база данных деструктивных контентов, появляющихся в региональных пабликах.
2. Непрерывно публикуется цикл статей, в том числе в иностранных журналах, а также – монографии, ориентированные на изучение процессов противоборства в социальных и корпоративных сетях, включая систематическую актуализацию РИП.
3. Запланировано ежегодное проведение научно-практической (с международным участием) конференции «Безопасный Интернет».

8. Рыночный потенциал продукта

8.1 Продукт

Основным продуктом является программно-технический комплекс мониторинга (ПТК) Интернет-публикаций для выявления деструктивного контента (ДК). Назначением данного продукта является отслеживание появления ДК в социальных сетях, а также средствах массовой информации, работающих в Интернете. Основной отличительной особенностью ПТК является использование целевой модели Интернет-пользователя, позволяющий ранжировать ДК по степени опасности и оперативно информировать пользователей ПТК о возникающих угрозах.

8.2 Рыночная ситуация

В данный момент времени в открытых источниках отсутствует информация о существующих программных комплексах мониторинга публикаций в сети Интернет с целью выявления ДК. Создаваемый ПТК может быть востребован федеральными и муниципальными органами государственной власти, а также общественными и коммерческими организациям. В первом случае ПТК может быть применен для оперативного информирования лиц принимающих решения в органах государственной власти об информационных вбросах, представляющих угрозы обществу и государству. Во втором случае ПТК применяется для выявления информационных атак на конкретные организации с целью подрыва их деловой репутации.

8.3 Конкурентная среда

Рассмотрим наиболее популярные в настоящий момент системы мониторинга и анализа социальных сетей. Система Radian 6 (www.radian6.com) предназначена для отслеживания в реальном времени упоминаний брендов с учетом тональности в социальных сетях (предоставляется панель управления мониторингом) и для участия в происходящих обсуждениях (предоставляется панель управления участием). Панель управления участием позволяет реагировать на активность в социальных сетях из одного места, используя имеющиеся учетные записи в блогах, площадках Twitter и Facebook. Для ретроспективного анализа доступны данные, накопленные за последние 30 дней. Такое ограничение представляется существенным для анали-

за продолжительных кампаний в социальных сетях. Заметим, что система Radian 6 в большей степени фокусируется на оперативном реагировании на происходящие события, нежели на бизнес-аналитике (стратегический уровень принятия решений), поэтому управляющие воздействия могут привести лишь к кратковременному всплеску продаж. Пользователям системы предоставляется возможность настраивать (и сохранять) профили ранжирования по следующим показателям: по количеству постов заданной темы, по количеству комментариев заданной тематики, по количеству уникальных комментаторов, по количеству входящих ссылок, по количеству голосов, по количеству ответов на тематических форумах.

Программный комплекс Radian 6 реализован на основе методов анализа и поиска текстов на уровне ключевых слов, анализа тональности текстов, а также визуального анализа. Недостатком Radian 6 является то, что данное программное обеспечение не использует математические методы анализа данных, а основывается лишь на лингвистических и графических методах.

Система мониторинга и анализа социальных сетей AlterianSM2. Основное решение компании SDL в области анализа социальных медиа – система Alterian SM2 в связке с дополнительными приложениями и сервисами. Система Alterian SM2 – типичная для своего класса система, которая позволяет отслеживать упоминания брендов в социальных сетях с учетом тональности (определяется положительная, отрицательная и нейтральная тональность). Кроме того, утверждается, что система позволяет локализовать места обсуждений и определять демографические характеристики пользователей социальных сетей.

Система анализа социальных сетей BrandSpotter позиционируется как система мониторинга и управления репутацией бренда в социальных сетях: отслеживаются упоминания бренда с учетом тональности; отслеживаются наиболее значимые пользователи социальных сетей по данной тематике (значимые с точки зрения количества упоминаний, тональности упоминаний, количеству последователей и друзей). Таким образом, система BrandSpotter предназначена для оценки текущей ситуации в социальных медиа и анализа данных за предыдущие периоды. При этом остается открытым вопрос прогнозирования развития ситуации.

Система анализа социальных сетей «Медиалогия» автоматически производит мониторинг и анализ сообщений более 92 миллионов источников социальных медиа. «Медиалогия» исследует все наиболее популярные платформы, включая Twitter, Facebook, Вконтакте, LiveJournal, Мой Мир, автономные блоги, а также специализированные форумы. Дополнительные источники подключаются по запросу. «Медиалогия» решает следующие задачи по мониторингу социальных медиа: оперативный мониторинг блогосферы и социальных медиа по заданным объектам и темам; отслеживание негатива и информационных рисков в блогах; определение наиболее популярных блогеров и сообществ; выявление наиболее активных и негативно настроенных блогеров; распределение упоминаний по площадкам, регионам, социально-демографическим показателям; анализ наиболее заметных инфоповодов; оценка охвата аудитории в соцмедиа; сравнение ключевых параметров присутствия в соцмедиа с конкурентами.

Программное обеспечение chotam.ru использует базовые методы поиска и анализа текстов на уровне ключевых слов. В случае, если вы являетесь администратором (модератором) или вам предоставили доступ, вы можете:

1. Отслеживать все посты, фотографии, видео и сообщения.
2. Получать уведомления, когда вам задали вопрос, через мессенджеры и электронную почту.
3. Сравнивать с другими подобными пабликами.
4. Отслеживать спам, быстро получать уведомления и ликвидировать вредонос.
5. Задавать вопрос эксперту и получать ответы на вопросы, связанные с мониторингом группы.

Единственная функция, доступная обычному пользователю, — это сортировка (фильтрация) комментариев по ключевым словам. Для этого надо:

1. Ввести слово/фразу в графу "сообщение содержит:"
2. Установить какому сервису принадлежит отслеживание.
3. Выбрать статус фильтрации (любой, одобрено, отфильтровано).
4. Выбрать тип. Из всех типов доступно произвести поиск только комментариев. Остальное (отзыв, пост, упоминание, сообщение, ответ, фото…) не работает.
5. Выбрать период, в который надо искать комментарии по ключевому слову/фразе.

Таким образом, ресурс chotam.ru весьма ограничен по своим структурно-функциональным возможностям.

Принципиальными недостатками всех вышеперечисленных систем являются:

- отсутствие ориентации их мониторинга на региональные паблики и каналы, существенно влияющие на общественное мнение в субъекте РФ;
- исключение из глубокого рассмотрения деструктивного контента (ДК), имеющего специфические особенности построения и признаки распознавания (на основе накопленной базы данных ДК и модели РИП);
- игнорирование возможностей риск-анализа процессов распространения ДК, включая соответствующую метрологию и прогнозирование ареала диффузии ДК в пабликах и каналах.

8.4 Доведение до потребителя, использование результатов

Прежде всего, через ученый совет РУНЦ представляется возможным демонстрировать для вероятных потребителей достоинства проекта. Это такие базовые для РУНЦ предприятия в регионе, как «Концерн «Созвездие», Государственный научно-исследовательский испытательный институт проблем технической защиты информации ФСТЭК России и др. Каналом информирования и взаимодействия можно также считать комиссию по информационной безопасности при губернаторе Воронежской области (руководитель проекта является ее членом), где представлены все региональные структуры, компетентные по данному профилю. Наконец, для связи с потребителями могут быть использованы ресурсы рабочей группы по развитию проекта «Безопасный Интернет», созданной приказом руководителя департамента образования, науки и

молодежной политики Воронежской области Мосолова О.Н. Исполнители проекта ежеквартально участвуют в заседаниях этой группы, регулярно выступают в СМИ и на сайте проекта безопасный-интернет.РФ.

Доведение до потребителя результатов проекта возможно также за счет адресной работы с муниципальными и региональными органами власти, вплоть до заключения с ними договоров о создании ситуационных центров реагирования на информационные атаки. Кроме этого, такая работа может быть осуществлена с частными предприятиями, заинтересованными в использовании разрабатываемого ПТК в своем бизнесе.

Важным ресурсом для доведения до потребителя результатов проекта следует считать дискуссионную площадку конференции «Безопасный Интернет».

8.5 Коммерческая и(или) социальная значимость ожидаемых результатов

Проект прежде всего ориентирован на школьную и студенческую молодежь региона – категорию населения Воронежской области, наиболее чувствительную к атакам деструктивного контента. В этом случае разрабатываемый ПТК имеет высокую социальную значимость с учетом возможностей его применения для обеспечения информационной безопасности региона и ограждения Интернет-пользователей от ДК посредством оперативного реагирования на эти атаки.

Коммерциализация проекта видится в двух направлениях:

1. Тиражирование научно-методических и программно-технических результатов проекта на другие субъекты РФ, заинтересованные в повышении информационной защищенности своих жителей от воздействия деструктивного контента. Органы власти этих регионов могли бы выступить заказчиками адаптации модели РИП и ПТК проекта в интересах населения своих территорий.
2. Настройка ПТК (под маркетинговые задачи) с целью мониторинга рынка по контентам с коммерческой перспективой, где заказчиками могли бы выступить заинтересованные в оперативном анализе негосударственные структуры. Здесь проявляется двойное назначение продукта, заключающееся в возможности настройки ПТК на выявление контента коммерческого свойства с последующим его исследованием (в интересах заказчика) в пространстве вероятной клиентуры.

9. Риски проекта

Одним из основных рисков для создаваемого ПТК является возможный эффект лавинообразного вброса деструктивных контентов, когда быстродействия может не хватить для выполнения необходимых процедур.

В этом случае от режима последовательного обхода пабликов придется перейти к распараллеливанию процессов мониторинга, увеличивающему быстродействие комплекса. Разумеется, заказчик в этом случае должен быть готов к дополнительным финансовым затратам на создание многоканальной аппаратной части ПТК, адекватной возможному всплеску контентной активности и перечню иссле-

дуемых региональных пабликов. Отсутствие учета этих факторов обуславливает возникающий в данном случае риск.

Минимизировать риск пропуска деструктивного контента при мониторинге пабликов возможно также за счет человеко-машинного подхода. Параллельно работающие студенческие кибер-отряды (в рамках научно-исследовательских, курсовых и дипломных работ) способны дополнительно наблюдать за региональным Интернет-пространством, содействуя совершенствованию ПТК в ходе его внедрения и эксплуатации.

10. Сведения об исполнителях проекта

Научная школа кафедры систем информационной безопасности ВГТУ включает 19 профессоров. Координаторами научной школы являются член-корреспонденты РАН Новиков Д.А. и Борисов В.И. Кафедра воспитывает 12 аспирантов и имеет свой диссертационный совет Д212.037.08 по специальности 05.13.19 «Методы и системы защиты информации, информационная безопасность».

Аспирантско-студенческое инновационное бюро (АСИБ) кафедры активно включилось в реализацию проекта. В частности, в рамках научно-исследовательской работы студенты сканируют региональные паблики и создают базу данных деструктивных контентов, выявленных в этих пабликах. Кроме того, АСИБ участвует в развитии и актуализации модели регионального Интернет-пользователя, проводит аналитические исследования этой модели в интересах региональной власти.

Результаты вышеуказанной работы в мае будут заслушаны на студенческой научной конференции «Социально безопасный Интернет». Наиболее продвинутые исследования планируется опубликовать в журнале «Информация и безопасность», издаваемом кафедрой систем информационной безопасности Воронежского государственного технического университета.

11. Мероприятия по информированию общественности о ходе и результатах выполнения исследований

Информирование общественности о ходе и результатах выполнения исследований проводится путем размещения соответствующей информации на официальных сайтах исполнителей проекта (ВГТУ и безопасный-интернет.рф). Ход развития проекта неоднократно освещался в СМИ («Аргументы и факты», ТНТ «Губерния»), что планируется делать и в последующем с учетом периодической отчетности исполнителей перед правительством Воронежской области РФ.

Исполнители намерены также активно взаимодействовать с общественными организациями, включая совместные действия по организации конференции и изданий с рабочим названием «Безопасный Интернет».

12. Перспективы развития проекта

Уже сейчас ведутся работы по расширению методологии мониторинга на социальные сети обмена медиа-контентом и соответствующие региональные каналы. В первую очередь это касается сетей YouTube и Instagram, для которых разрабатываются риск-метрики и алгоритмы распознавания ДК, формируется РРДК.