

# Безопасный Интернет

Руководитель проекта:

руководитель Регионального учебно-научного центра по  
проблемам информационной безопасности (РУНЦ),  
заведующий кафедрой систем информационной безопасности

Воронежского государственного технического университета

Остапенко Александр Григорьевич

E-mail: [mnac@comch.ru](mailto:mnac@comch.ru); [kafedrasib.ru](mailto:kafedrasib.ru)

## Цель и задачи проекта

**Цель:** повышение информационно-психологической защищенности жителей Воронежской области Российской Федерации, пользующихся услугами социальных сетей, в условиях массированного воздействия на них деструктивного контента.

### Задачи

Формирование модели регионального Интернет-пользователя на основе социологического опроса различных категорий населения и статистического анализа их информационных предпочтений

Разработка и внедрение лектория, популяризирующего в школах и университетах региона проблему обеспечения безопасности Интернет-пространства

Создание инструментария автоматизации процедур выявления и прогнозирования диффузии деструктивного контента в Интернет-сегменте региона

Внедрение созданного инструментария в лекторий проекта и в органы власти в качестве средств поддержки принятия управленческих решений в ходе информационного противоборства. Интеграция проекта с созвучными программами России и СНГ, включая тиражирование результатов проекта в других субъектах РФ

### Средства достижения цели

Научная школа РУНЦ (2 член-корреспондента РАН, 21 доктор наук), конференция «Безопасный Интернет», а также издаваемый ВГТУ журнал (в перечне ВАК России) «Информация и безопасность»

Реализуемые РУНЦ в регионе программы подготовки специалистов и кадров высшей квалификации в области информационной безопасности (аспирантура и диссовет при РУНЦ)

Регулярные опросы критичных групп Интернет – пользователей региона по вопросам распространения деструктивного контента в социальных сетях (с привлечением социологов и психологов)

Методические, алгоритмические и программные наработки РУНЦ и Воронежского научно-образовательного центра управления информационными рисками (создан ВГТУ совместно с РАН) в области дискретного моделирования эпидемических процессов в гетерогенных сетях (за последние 5 лет опубликовано 10 монографий, свыше 100 отечественных и 30 зарубежных статей)

<p>Интернет-ресурсы <i>Социальные сети</i></p> <p>Арена антагонистического противоборства за право информационного управления личностью и социумом</p>	<p>Интернет- контент <i>Деструктивный контент</i></p> <p>Ориентирован на информационно-психологическую дестабилизацию и дезорганизацию личности и социума</p>	<p>Региональный Интернет - пользователь <i>Критичные социальные группы</i></p> <p>Школьники и студенты, особенно восприимчивые к деструктивному контенту, включая их сообщества в социальных сетях</p>
--	---	--

## Ожидаемые результаты проекта

<p>2017 год</p>	<p>Апробированные на организуемой конференции «Безопасный Интернет» предпроектные заделы. Зарубежные (WoS, SCOPUS) и отечественные (ВАК) – публикации их материалов, включая издание монографий серии «Теория сетевых войн». Сайт проекта. Модель регионального Интернет-пользователя под воздействием информационных угроз. Региональная рабочая группа проекта (РРГП). Обсужденные на ее заседаниях результаты опроса и задание на 2018 год.</p>
<p>2018 год</p>	<p>Программно-технические комплексы (ПТК) выявления и прогнозирования процессов распространения деструктивного контента в Интернет – пространстве региона. Учебный класс и проектный офис. Актуализированная модель пользователя. Лекторий «Сетевое противоборство и безопасный Интернет» в школах и университетах региона. Апробированные и опубликованные результаты. На заседании РРГП утвержденное задание на 2019 г.</p>
<p>2019 год</p>	<p>Актуализированные и адаптированные ПТК проекта, внедренные в учебный процесс и практику государственного и муниципального управления. Обученные пользователи ПТК. Интеграция проекта в созвучные федеральные программы. Демонстрационная версия методического и программного обеспечения проекта для тиражирования его результатов на другие субъекты РФ. Апробированные и опубликованные результаты. Обсужденные на заседании РРГП итоги проекта и пути его развития.</p>

## Влияние проекта на регион

Инициаторами проекта выступили **первый заместитель председателя Правительства Воронежской области Попов В.Б. и ректор Воронежского государственного технического университета (ВГТУ) Колодяжный С.А.**, исходя из предпроектного задания Регионального учебно-научного центра по проблемам информационной безопасности (РУНЦ), созданного в рамках ВГТУ по приказу Минобра РФ ( № 11781 от 20.08.1997 г.).

Для координации проекта создана региональная рабочая группа, которую возглавил **руководитель департамента образования, науки и молодежной политики Воронежской области О.Н. Мосолов** ( приказ № 1152 от 03.10.2017 г.).

В проект включаются и вошли в состав Ученого совета РУНЦ доктора наук - представители руководства :

Департамента связи и массовых коммуникаций Воронежской области;

Аппарата Уполномоченного по правам человека по Воронежской области;

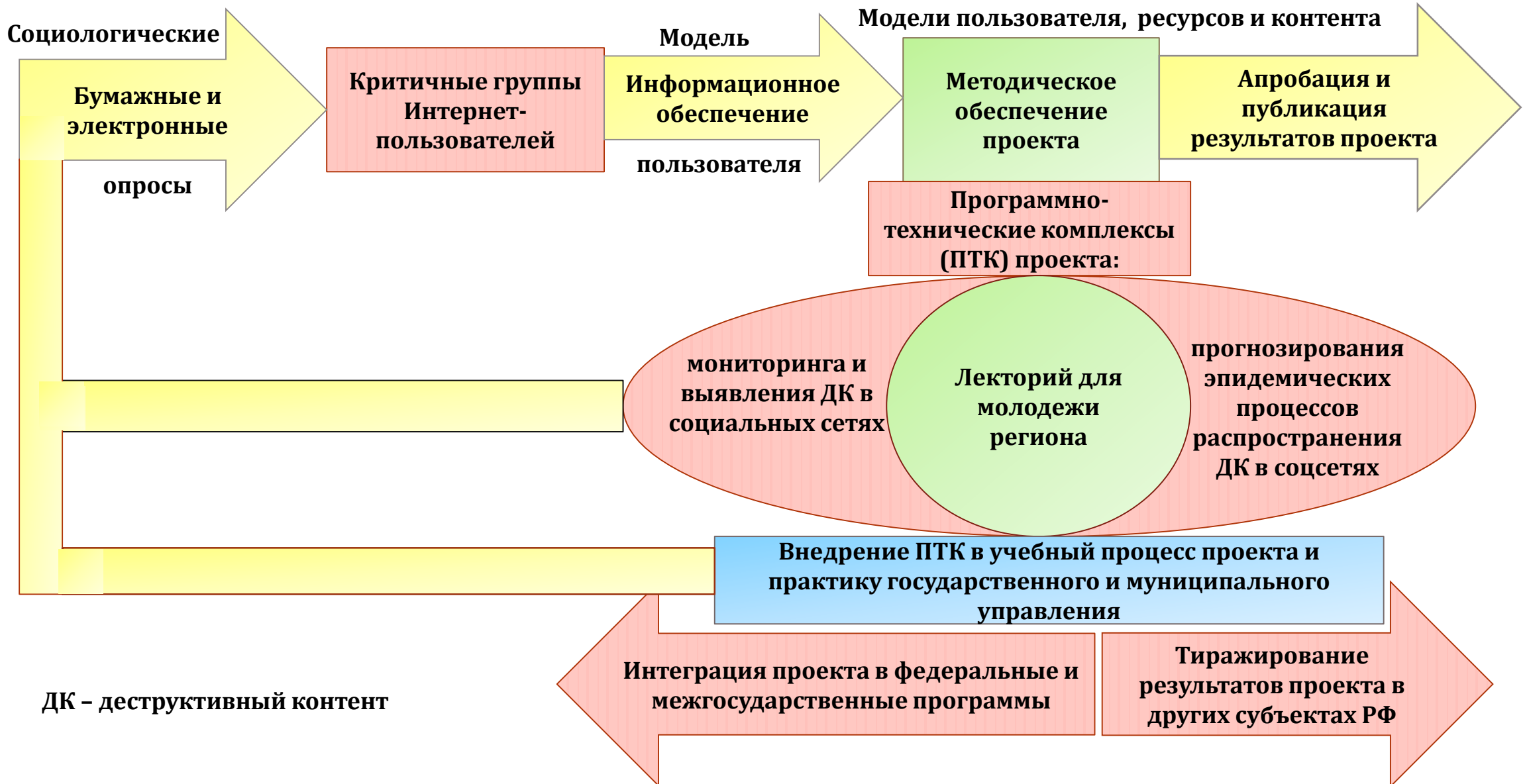
АО «Концерн «Созвездие» (г. Воронеж);

Государственного научно-исследовательского испытательного института проблем технической защиты информации (г. Воронеж).

**Пользователи результатов проекта:** учебный процесс ВГТУ по специальностям в сфере обеспечения информационной безопасности. Органы власти, ситуационные центры, озабоченные обеспечением Интернет-безопасности в региональном социуме. В IV квартале 2017 года под проект выделено стартовое финансирование в размере 1750 тыс. рублей.

**Рынки сбыта:** субъекты РФ и их муниципальные образования, население которых подвергается массированному деструктивному информационному воздействию через сеть Интернет.

# Структура проекта



## Структура модели пользователя



### Оригинальность:

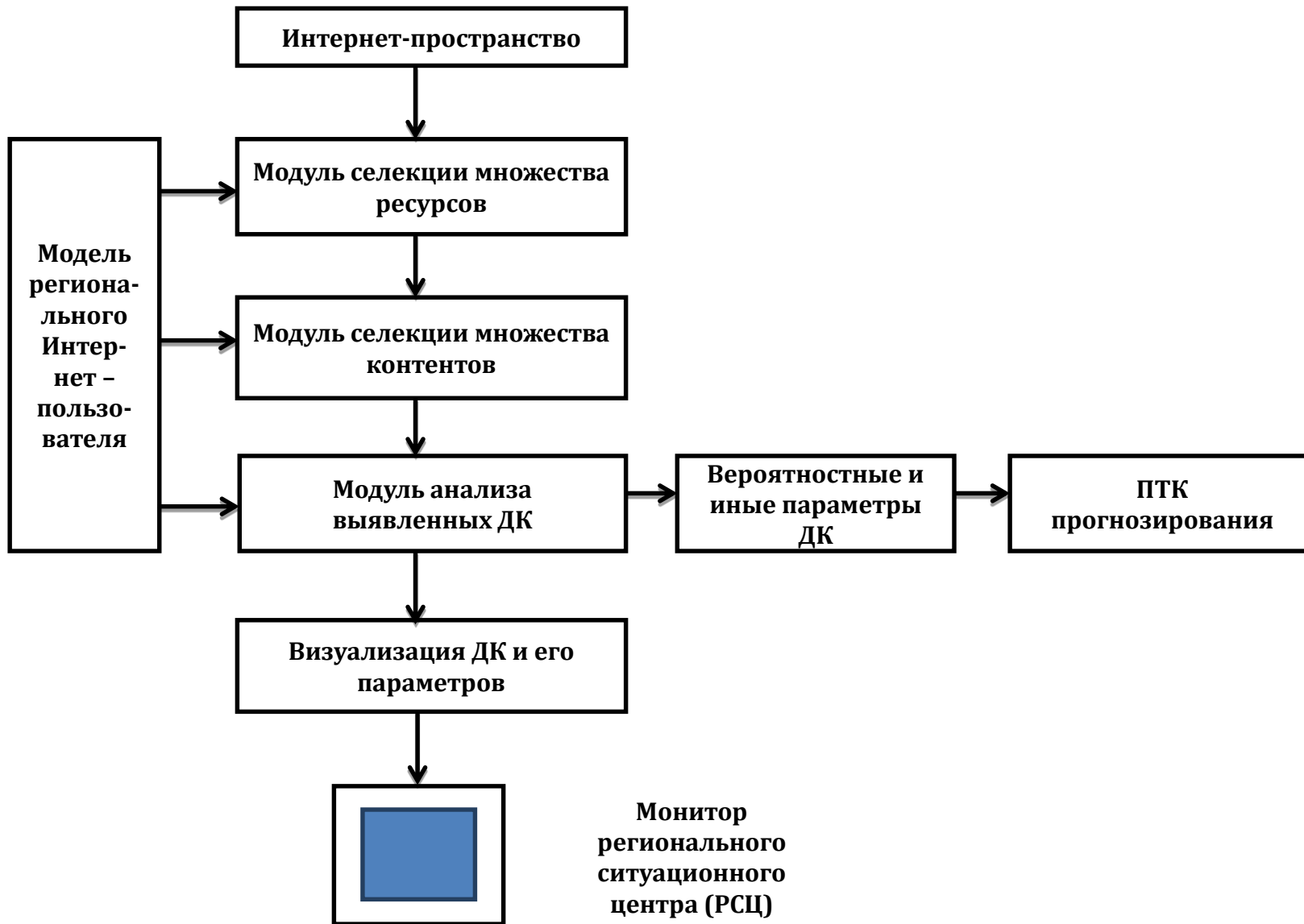
- В отличие от аналогов, модель имеет **социальную направленность**, и учитывает ментальность его жителей.
- С помощью периодических опросов модель имеет **возможность подстраиваться** под изменения в предпочтениях Интернет-пользователя региона.
- Модель регионального пользователя **позволяет маркировать ресурсы и контент** по предпочтениям регионального пользователя.

### Сервисные возможности:

- Пользователь РСЦ по любому срезу (мужчины, 20-25 лет, среднего достатка и др.) может **узнать соответствующие ему информационные предпочтения** (сети, сообщества, контент и др.).
- Пользователь РСЦ может для выявленного ДК **определить возможный ареал его распространения** в региональном Интернет-пространстве.

# Структура программно-технического комплекса (ПТК) мониторинга

7



## Оригинальность:

В отличие от аналогов, данный программно-технический комплекс позволяет:

- Проводить **внешний мониторинг** популярности ДК, **без необходимости внедрения стороннего кода** на анализируемый ресурс.
- **Автоматизировать выявление деструктивного контента** по информационно-социальным моделям пользователя.
- Имеет **гибкую систему ранжирования ДК** по степени опасности (оценка вероятностей заражения, иммунизации, излечения и т.п. пользователя).

## Сервисные возможности:

- Пользователь ПТК мониторинга на экране РСЦ имеет возможность **визуализировать ДК и его параметры**.
- ПТК мониторинга передаёт **вероятностные параметры ДК** на ПТК прогнозирования.

# Структура программно-технического комплекса (ПТК) прогнозирования



## Оригинальность:

- В отличие от эпидемических аналогов ПТК, базируется на дискретных моделях (состояния пользователя дискретны), позволяющих по-шагово прогнозировать диффузию ДК в социальных сетях.
- В основу положено **послойное представление весьма неоднородных (гетерогенных) социальных сетей.**
- Предусмотрено развитие ПТК на задачи **прогнозирования процессов противоборства контентов** в социальных сетях.

## Сервисные возможности:

- Пользователь РСЦ имеет возможность **визуально наблюдать прогноз** по шагам распространения ДК в любой социальной сети, представляющей интерес для исследователя.
- По параметрам выявленного ДК и модели пользователя РСЦ представляется возможным **определить категории пользователей, к которым может попасть ДК.**



## Сущность продуктов проекта

*Гигантские размеры территории и многонациональный состав России обусловили специфические интеллектуальные, эмоциональные, культурные, ценностные ориентации и установки, свойственные ее регионам. Это проявляется и в специфике облика регионального Интернет-пользователя.*

**Модель пользователя** формируется на основе статистической обработки результатов социологических опросов (бумажных, электронных), проводимых по данному РРГП формату. При этом автоматизированная модель должна позволять по выявленному ДК (его виду, тематике и т.п.) определять возможный ареал его распространения в разрезе различных категорий жителей регионов. Оболочка программной реализации модели обязана быть открыта для модернизации (развитию базы вопросов и т.п.), а также – к последующему анализу динамики модели в контексте развития стремительно меняющегося информационного общества. Программная реализация модели обязана обеспечить выявление информационных предпочтений отдельных слоев регионального пользователя.

## Сущность продуктов проекта

В отношении **ПТК мониторинга** модель должна предоставлять возможность отбора Интернет-ресурсов, подлежащих первоочередному сканированию на предмет поиска набирающего популярность ДК. Краеугольное значение в этой связи имеют процедуры идентификации контента в качестве деструктивного, где должно быть разработано специальное математическое обеспечение и критериальная основа отбора всевозможных разновидностей контента (текстового, видео и др.). На основе разработанного математического и алгоритмического обеспечения будет создано ПО для ранжирования угроз с возможностью визуализации результатов мониторинга в режиме реального времени.

Исходными данными для **ПТК прогнозирования** служат находящиеся в открытом доступе параметры топологии и трафика социальных сетей, а также вероятности восприятия ДК, определенные ПТК мониторинга. При этом ареал ДК, определенный из модели пользователя, указывает ПТК на возможные источники инфицирования. Выходными данными ПТК прогнозирования следует считать пошаговую визуализацию процесса диффузии ДК, выявленного в социальной сети. Для выполнения вышеуказанных процедур потребуется разработка специального математического обеспечения.

*Лекторий проекта должен соответствовать модели пользователя и систематически актуализироваться с учетом результатов проекта и выявленных ДК, а также – динамики предпочтений региональной молодежи.*