

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГТУ», ВГТУ)

Программно-технический комплекс «Безопасный Интернет»

Ректор ВУЗа _____ С.А. Колодяжный
Подпись

Секретарь научно-технического совета _____ С.М. Усачев
Подпись

Автор _____ Е.А. Шварцкопф
Подпись

Воронеж
2017

ОПИСАНИЕ ИННОВАЦИОННОГО ПРОЕКТА

1. Содержание	
2. Ключевые слова.....	3
3. Актуальность и востребованность результатов проекта	4
3.1 Описание продукции (технологии).....	4
3.2 Анализ наличия на рынке аналогов, имеющих сопоставимые технические и эксплуатационные характеристики	4
3.3 Анализ потребностей рынка (ниши и масштабы).....	5
3.4 Наличие заказчика(-ов) продукции, технологии	6
4. Коммерциализация проекта	7
4.1 Наличие опытного образца, действующей модели.....	7
4.2 Экономическая эффективность инновационного проекта.....	7
4.3 Анализ себестоимости производства продукции (эффективности технологии) по сопоставимым аналогам.....	8
4.4 Обоснованность плана коммерциализации инновационного проекта, результаты освоения в производстве, результаты собственной коммерциализации проекта	8
4.5 Предложения по привлечению финансовых средств (использования собственных средств, средств внешних инвесторов, в том числе инвестиционных кредитов банков и т.д.).....	9
4.6 Уровень проработки маркетинговой стратегии	10
4.7 Риски коммерциализации	10
5. Научно-техническая проработка инновационного проекта	12
5.1 Научно-техническое обоснование технических решений, идей	12
5.2 Оценка степени влияния неучтенных факторов на достижение практических результатов.....	14
5.3 Результаты лабораторных, исследовательских работ, заложенных в основу технических решений.....	14
6. Патентоспособность.....	26

6.1 Наличие патента, заявки на техническое решение, плана действий по защите прав на интеллектуальную собственность.....	26
6.2 Патентная чистота, качество патентного поиска (проверка новизны и наличия ближайших аналогов).....	26
7. Значимость проекта.....	28
7.1 Влияние на рост уровня и повышение качества жизни населения	28
7.2 Влияние на безопасность населения.....	29
7.3 Создание конкурентоспособного, высокотехнологичного промышленного комплекса в регионе	30
7.4 Формирование условий для использования научно-технического потенциала воронежской области в целях повышения конкурентоспособности промышленности	30

2. КЛЮЧЕВЫЕ СЛОВА

Программное обеспечение, сеть, модели, контент, анализ, моделирование, эпидемии.

3. АКТУАЛЬНОСТЬ И ВОСТРЕБОВАННОСТЬ РЕЗУЛЬТАТОВ ПРОЕКТА

3.1 ОПИСАНИЕ ПРОДУКЦИИ (ТЕХНОЛОГИИ)

Программно-технический комплекс «Безопасный Интернет» (далее - Проект) - это сервис для анализа актуальных процессов и трендов в сети Интернет с точки зрения общественной безопасности (федеральный, региональный, местный уровень).

3.2 АНАЛИЗ НАЛИЧИЯ НА РЫНКЕ АНАЛОГОВ, ИМЕЮЩИХ СОПОСТАВИМЫЕ ТЕХНИЧЕСКИЕ И ЭКСПЛУАТАЦИОННЫЕ ХАРАКТЕРИСТИКИ

Аналогами данного программно-аппаратного комплекса следует считать программный комплекс: ПРИЗМА (ООО «Медialogия»). «ПРИЗМА» - ПО предназначенное для управления репутацией и рисками в социальных медиа. Она помогает оперативно отслеживает в соцмедиа активности, приводящие к росту социальной напряжённости и анализирует интерес блогосферы к тем или иным проблемам и предупреждает о возможных репутационных рисках. ПРИЗМА может быть оперативно развёрнута в течение нескольких дней. Клиентская часть решения — брендированный моноблок с предустановленным программным обеспечением. Т.е. стоимость ПРИЗМЫ состоит из стоимости моноблока, программного обеспечения и обслуживания. За счет необходимости приобретения моноблока стоимость программного продукта резко увеличивается. Разрабатываемый нами программный комплекс реализован по модели SaaS , т.е. доступ к программному обеспечению через Интернет, приобретение дорогостоящего оборудования для пользователей нашего ресурса не потребуется. Проверка выигранных «Медialogией» и связанной с ней компанией «Медиамониторинг» (зарегистрирована по тому же адресу)

тендеров по сайту госзакупок показала: поставок «Призмы» кому-либо из госзаказчиков в 2011-2012 годах не было (всего 14 побед в госконкурсах).

Система использует только несколько сотен блогеров, и анализирует то, что происходит внутри их замкнутого сообщества. Это слишком малая часть, она не дает представления об общей картине. Необходимо понимать, что в реальном времени происходит в сетях. Необходимы разработки по манипулированию этой средой, используя модели распространения информации в социальных сетях в зависимости от характера новости и репутации «агента». Преимущество нашего программного комплекса «Netepidemic» заключается в возможности моделирования и прогнозирования эпидемий, определения наиболее вероятных объектов атаки в сети, что позволяет провести оценку эффективности тех или иных мер противодействия распространения эпидемии.

Компания "Медialogия" пять лет работает на рынке обработки информации. Ее система анализа и мониторинга данных возникла как внутренний проект российского холдинга IBS (разработка и внедрение ИТ-решений, сервис в области ИТ). Утверждается, что в разработку системы было вложено около 10 млн долларов. Сначала обработка данных велась в основном вручную, потом большая часть операций (85–90%) была автоматизирована.

Пока стратегия "Медialogии" была достаточно успешной - бизнес растет практически на 100% ежегодно. Сама компания свои обороты не раскрывает, но, по оценкам некоторых экспертов, они могут составлять до 10–15 млн долларов в год. При этом общий объем российского рынка анализа СМИ составляет, по оценкам, 60–100 млн долларов.

3.3 АНАЛИЗ ПОТРЕБНОСТЕЙ РЫНКА (НИШИ И МАСШТАБЫ)

Объемы рынка социальных сетей можно оценить, как бездонные и по причине того, что программный комплекс не ограничен никакими определенными тематиками и не имеет привязки к конкретной социальной

сети, точно оценить объем рынка достаточно сложно. Однако учитывая ежемесячную активную аудиторию только российских социальных сетей более 150млн. Можно предположить, что при грамотном продвижении продукта, как помощи для поиска перспективных направлений в определенной аудитории, принесет не менее 30-40 млн.руб. в первый год.

3.4 НАЛИЧИЕ ЗАКАЗЧИКА(-ОВ) ПРОДУКЦИИ, ТЕХНОЛОГИИ

Разработанное программное средство может использоваться в учебном процессе технических вузов при изучении дисциплины «Социальные сети: риски и обеспечение безопасности». Проект разрабатывался в рамках региональной программы «Безопасный Интернет». Стартовая версия программно-технического комплекса «Безопасный Интернет» и информационных рисков в структуре населения Воронежской области потенциально интересна Вузам региона, Воронежскому научно-образовательному центру управления информационными рисками, региональным органам власти и территориальным органам компетентных федеральных ведомств.

4. КОММЕРЦИАЛИЗАЦИЯ ПРОЕКТА

4.1 НАЛИЧИЕ ОПЫТНОГО ОБРАЗЦА, ДЕЙСТВУЮЩЕЙ МОДЕЛИ

Разработана стартовая версия на базе кафедры систем информационной безопасности, которая прошла апробацию в Воронежском государственном техническом университете и получила одобрение специалистов в области защиты информации (от Государственного научно-исследовательского испытательного института проблем технической защиты информации ФСТЭК России, АО «Концерн «Созвездие»» и Института проблем управления РАН).

Эффективность программы (по критерию цена/качество) может быть существенно повышена при опоре на профессорско-аспирантско-студенческие творческие коллективы, мотивированные на исследование социальных информационных сетей и управление региональными социотехническими системами. Примером этому может служить аспирантско-студенческое инновационное бюро кафедры систем информационной безопасности Воронежского государственного технического университета (ВГТУ), в инициативном порядке разработавшее программно-технический комплекс прогнозирования процессов распространения деструктивного контента в социальных сетях «Netepidemic».

4.2 ЭКОНОМИЧЕСКАЯ ЭФФЕКТИВНОСТЬ ИННОВАЦИОННОГО ПРОЕКТА

Программный комплекс для моделирования развития вирусных эпидемий находится в заключительной стадии разработки, поэтому далее будут представлены планируемые экономические показатели.

1) Объем продаж (в т.ч. планируемый): Планируется выпускать до 100 копий продукции в год

2) Выручка от реализации (в т.ч. планируемая): Выручка от реализации продукции 50 тыс. руб. в год

3) Валовые затраты, прямые и переменные.

Наименование статей затрат	Сумма, р.
1. Основные материалы, покупные изделия и полуфабрикаты	–
2. Затраты на покупку и аренду спецоборудования	39000
3. Основная заработная плата исполнителей	12 636
4. Дополнительная заработная плата исполнителей	–
5. Отчисления на социальные нужды	–
6. Внепроизводственные расходы	–
7. Прочие прямые расходы	–
8. Накладные расходы	–
Полная себестоимость	51 636

4) Налоговые поступления в бюджеты всех уровней.

Налоговые поступления в бюджет составят 6,5 тыс. руб. в год рублей в год.

4.3 АНАЛИЗ СЕБЕСТОИМОСТИ ПРОИЗВОДСТВА ПРОДУКЦИИ (ЭФФЕКТИВНОСТИ ТЕХНОЛОГИИ) ПО СОПОСТАВИМЫМ АНАЛОГАМ

Полная себестоимость 51 636.

4.4 ОБОСНОВАННОСТЬ ПЛАНА КОММЕРЦИАЛИЗАЦИИ ИННОВАЦИОННОГО ПРОЕКТА, РЕЗУЛЬТАТЫ ОСВОЕНИЯ В ПРОИЗВОДСТВЕ, РЕЗУЛЬТАТЫ СОБСТВЕННОЙ КОММЕРЦИАЛИЗАЦИИ ПРОЕКТА

Основываясь на том, что заказчиками инструментария управления Интернет-рисками Воронежской области будут являться Вузы региона, необходимо постоянно вести работу с руководством данных учреждений. Так же занятию данной ниши рынка способствует тот факт, что программный

комплекс разрабатывался в рамках региональной программы «Безопасный интернет» и не имеет полных аналогов, которые бы повторяли весь основной функционал. Особенно данный продукт будет интересен Воронежскому научно-образовательному центру управления информационными рисками, УФСБ и ГУВД по Воронежской области.

С использованием SbS модели можно рассчитывать на полноценный охват рынка. Конфигуратор программного комплекса будет включать в себя, как отдельные модули по различному анализу информационных воздействий, так и будет учитываться количество выполняемых операций за расчетный период. Это позволит наиболее гибко предоставлять пользователям нужный функционал.

Возможность публикации статей в журнале SIB, имеющим статус ВАК и обладающим обширной базой подписчиков, о различных исследованиях, основанных на результатах, полученных при помощи программно-технического комплекса «Безопасный Интернет», создаст постоянный спрос и интерес к продукту. Журнал популярен среди людей, наиболее близких к вопросу защиты ИБ, это позволит программному комплексу, приобрести статус доверенного продукта.

4.5 ПРЕДЛОЖЕНИЯ ПО ПРИВЛЕЧЕНИЮ ФИНАНСОВЫХ СРЕДСТВ (ИСПОЛЬЗОВАНИЯ СОБСТВЕННЫХ СРЕДСТВ, СРЕДСТВ ВНЕШНИХ ИНВЕСТИТОРОВ, В ТОМ ЧИСЛЕ ИНВЕСТИЦИОННЫХ КРЕДИТОВ БАНКОВ И Т.Д.)

Собственные инвестиции. Формирование заявок на получение инвестиций в Сколково. Разработка бизнес-плана и презентаций проекта (состав решения, отличия от конкурентов). Демонстрация документов потенциальным инвесторам. Источниками финансирования программы предполагаются федеральный и региональный бюджеты.

4.6 УРОВЕНЬ ПРОРАБОТКИ МАРКЕТИНГОВОЙ СТРАТЕГИИ

Отвечая на вопрос кому выгоден данный продукт, стоит заметить, что рынок его применения довольно широк:

Для крупных компаний анализ перспективности предстоящего запуска нового товара или сезонной акции легко может быть смоделировано на малой аудитории, исходя из полученных результатов можно сделать выводы и изменить коммерческое предложение.

Для аналитических агентств можно проанализировать уже существующие посты и информационные «вбросы» по конкретным тематикам и ключевым словам. Это позволит увидеть перспективность отдельных отраслей и предложений.

Для отдельных пользователей, программный комплекс не менее ценен. Он позволяет сделать статистическую выгрузку по требуемой тематике за период времени. Это полезно в тех случаях, когда надо предоставить статистику популярности за выбранный временной промежуток и построить график динамики изменений.

С точки зрения обеспечения безопасности и контроля отдельных тем и деструктивных воздействий для простого обывателя будет предложен весь функционал анализа полученных данных.

4.7 РИСКИ КОММЕРЦИАЛИЗАЦИИ

Благодаря современному интересу к эпидемиологии связанном, в частности, с развитием компьютерных технологий и участвовавшими случаями заражения компьютерными вирусами риски, связанные с экономическим спадом, имеют место быть только в результате насыщения рынка (узкий профиль организаций для распространения). Но с другой стороны резкого спада в спросе на продукцию не ожидается, так как планируется постоянно вести инновационные поиски, исследования в данной области, что должно привести,

в конечном счёте, к обновлению, дополнению ПО. Риски от пожаров, ураганов, хищений и других подобных обстоятельств, включая землетрясение, будут покрыты обычными страховыми полисами. Возможны, однако, риски, связанные с различными источниками их возникновения.

Коммерческие риски: риск, связанный с реализацией товара, риск, связанный с перевозкой или транспортный риск, риск, связанный с приемкой товара покупателем.

Политические риски: риск, связанный с забастовками во время перевозки товара покупателю.

Источники возникновения рисков: недостаточная информация о спросе на данный товар, недостаточный анализ рынка и недооценка своих конкурентов.

Действие перечисленных рисков будут незначительны вследствие работы только после строгой проверки финансового положения и репутации будущего клиента.

5. НАУЧНО-ТЕХНИЧЕСКАЯ ПРОРАБОТКА ИННОВАЦИОННОГО ПРОЕКТА

5.1 НАУЧНО-ТЕХНИЧЕСКОЕ ОБОСНОВАНИЕ ТЕХНИЧЕСКИХ РЕШЕНИЙ, ИДЕЙ

Проект разрабатывался в соответствии с этапами:

1. На основе психоанализа и социологических исследований:

- выявление Интернет-предпочтений, устремлений и ожиданий различных категорий и групп населения;

- установление популярности и режима пользования для Интернет-ресурсов, востребованных различными категориями и группами населения области;

- вероятностная оценка восприятия и распространения разнообразного по содержанию и форме контента, циркулирующего в интернет-пространстве, для соответствующих категорий и групп населения региона.

2. На основе разработанной модели регионального Интернет-пользователя:

- исследование Интернет-ресурсов, используемых жителями области, в контексте обеспечения информационной безопасности личности и общества;

- выявление угроз нарушения региональной Интернет-безопасности для различных категорий и групп населения области;

- оценка риска реализации выявленных информационных угроз в отношении населения региона.

3. На основе разработанных моделей:

- формирование информационного обеспечения, необходимого для их программной реализации;

- разработка математического обеспечения для моделирования Интернет-отношений и информационных рисков в структуре населения региона;

- создание алгоритмического обеспечения для реализации, программно-технического комплекса Интернет-моделирования.

4. В соответствии с разработанными алгоритмами:

- выбор необходимого лингвистического обеспечения, необходимого для их программной реализации;

- создание программно-технического комплекса «Безопасный Интернет» и информационных рисков в структуре населения региона;

- тестирование и коррекция стартовой версии программно-технического комплекса Интернет-моделирования.

5. С учетом рекомендаций региональных органов власти и территориальных органов заинтересованных федеральных ведомств:

- модернизация стартовой версии программно-технического комплекса «Безопасный Интернет» и информационных рисков в структуре населения региона;

- проведение межрегиональной научно-практической конференции по тематике программы и результатам проведенных в ней исследований и реализованных разработок;

- публикация результатов работы и открытие соответствующих образовательных программ.

6. Создание инструментария управления информационными рисками (с использованием разработанного программно-технического комплекса), включая:

- прогнозирование деструктивных Интернет-процессов в структуре населения региона;

- рекомендации и методики противодействия Интернет-угрозам, реализуемым в отношении жителей области;

- их практическое внедрение в реальных информационных контрмерах, реализуемых совместно с компетентными органами власти на территории области.

5.2 ОЦЕНКА СТЕПЕНИ ВЛИЯНИЯ НЕУЧТЕННЫХ ФАКТОРОВ НА ДОСТИЖЕНИЕ ПРАКТИЧЕСКИХ РЕЗУЛЬТАТОВ

Неучтенные факторы это постоянно меняющаяся экономическая и политическая конъюнктура, а также кризис. Представляется сложным предопределить, как могут сказаться данные факторы на сбыт программного комплекса.

5.3 РЕЗУЛЬТАТЫ ЛАБОРАТОРНЫХ, ИССЛЕДОВАТЕЛЬСКИХ РАБОТ, ЗАЛОЖЕННЫХ В ОСНОВУ ТЕХНИЧЕСКИХ РЕШЕНИЙ

Разработанный программный комплекс построен по клиент-серверной технологии и представляет собой веб-приложение, базирующееся на платформе .NET. Данная платформа поставляется вместе со свободно распространяемым фреймворком ASP.NET MVC 5, использованным при написании программного комплекса.

ASP.NET (Active Server Pages для .NET) — технология создания веб-приложений и веб-сервисов от компании Майкрософт.

Помимо использования .NET – технологий, в работе использованы также другие технологии для введения дополнительных возможностей в функционал системы.

Основным требованиями к технологиям являлись их бесплатность и возможность использования в разработке веб-интерфейсов. Далее приводится краткий обзор используемых в приложении технологий, а также описание структуры программы.

Программный комплекс по своему функциональному назначению разделен на три больших функциональных компонента (MVC), каждый из которых отвечает за определенную часть функционала. Подобное структурное разделение обеспечивает слабосвязанную архитектуру, что обеспечивает широкие возможности по расширяемости и масштабируемости приложения.

Функциональное взаимодействие удобно отображать с помощью блоковой архитектуры. Рассмотрим взаимодействие элементов каждого из компонентов приложения.

На рисунке 1 представлено стартовое окно программы, в которое включены некоторые исправления, внедренные после модернизации разрабатываемого ПО. Исправления включают: флажок учета динамики во время эпидемического процесса, поле ввода коэффициента прироста сети на каждом шаге, кнопки «Сохранить изображение» и «Изменить размер полотна», также, флажок (скрыт в параметрах) с возможностью удаления вспомогательных линий-слоев с послойной модели и указатель направления растягивания полотна, содержащего изображение графа.

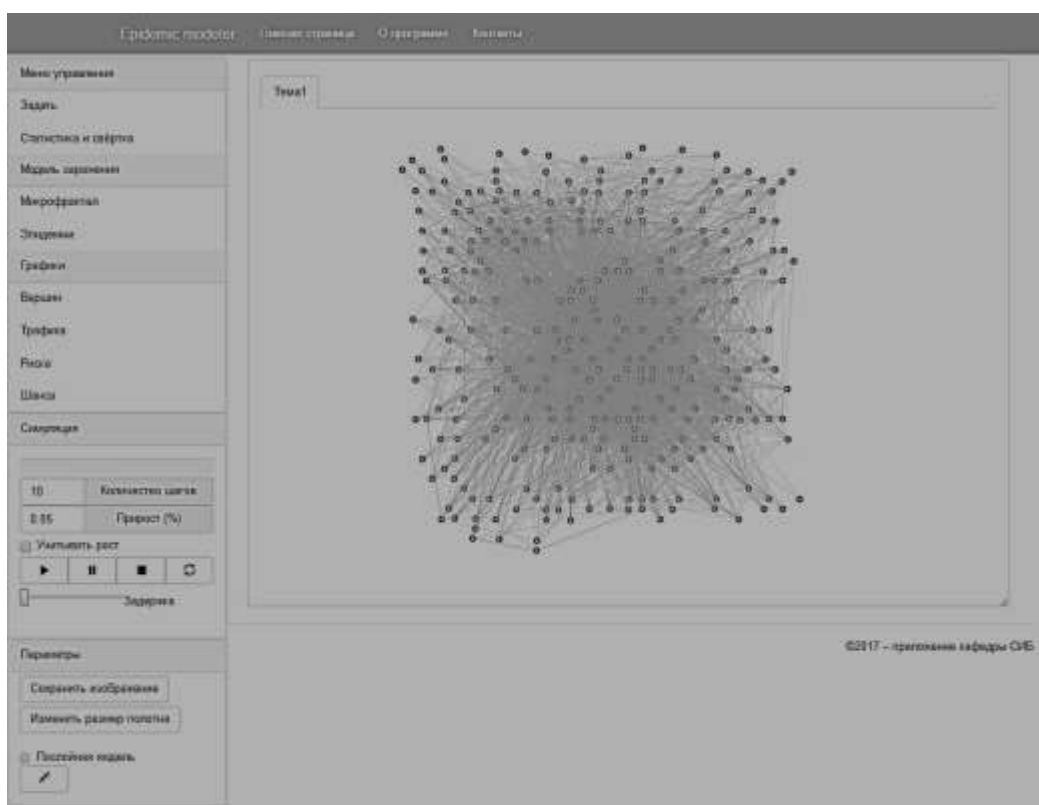


Рисунок 1 – Стартовое окно программы имитационного моделирования атак

Рисунок 2 включает в себя изображение блока «Симуляция», в который были добавлены флажок учета роста сети при эпидемическом процессе и поле ввода коэффициента прироста сети на каждом шаге. При переключении флажка учета роста вызывается следующая функция, где с помощью библиотеки jQuery

логической переменной (флаг) *isSetGrowth* присваивается значение, соответствующее свойству *checked* объекта с идентификатором *checkGrowth* (флажка учета роста).

```
1 //checkbox Учитывать рост
2 this.toggleGrowth = function ()
3 {
4     isSetGrowth = $('#checkGrowth').prop('checked');
5 }
```

В блоке «Параметры» (рис. 2) теперь присутствует кнопка «Сохранить изображение», с помощью которой появилась возможность сохранить изображение всего поля для вывода графа без установки дополнительного ПО.

После нажатия на эту кнопку вызывается функция *SaveSVG()*, имеющая следующий javascript-код:

```
1 function SaveSVG() {
2     var svg = document.querySelector('svg');
3     var canvas = document.createElement('canvas');
4     canvas.height = svg.getAttribute('height');
5     canvas.width = svg.getAttribute('width');
6     canvvg(canvas, svg.parentNode.innerHTML.trim());
7     var dataURL = canvas.toDataURL('image/png');
8     var data = atob(dataURL.substring('data:image/png;base64,',.length)),
9     asArray = new Uint8Array(data.length);
10    for (var i = 0, len = data.length; i < len; ++i) {
11        asArray[i] = data.charCodeAt(i);
12    }
13    var blob = new Blob([asArray.buffer], {type: 'image/png'});
14    saveAs(blob, 'export_' + Date.now() + '.png');
15 };
```

Здесь в переменную *svg* записывается содержимое *svg*-контейнера (поля с изображением графа), создается полотно *canvas*, отличное от *svg*-контейнера тем, что оно использует растровое изображение, параметры высоты и ширины полотна соответствуют текущим параметрам *svg*-контейнера. Затем с помощью функции *canvvg()* из сторонней библиотеки *canvg* выполняется преобразование векторного содержимого *svg*-контейнера в растровое изображение для *canvas*. Далее происходит преобразование форматов, и функцией *saveAs()* из сторонней библиотеки *FileSaver.js* файл с уникальным именем (текущая дата и время) сохраняется на компьютер.

Также, здесь есть кнопка «Изменить размер полотна», которая устанавливает размеры контейнера с SVG-графикой, содержащего граф, в соответствии с тем размером поля, которое необходимо пользователю (изменяется после растягивания поля указателем).

При нажатии на эту кнопку вызывается функция *ChangeSize()*, имеющая следующий код:

```
1 function SaveSVG()
2 {
3     var pan_pandef_res = document.querySelector('.panel.panel-default.resizable'); //parent -
4     this
5     var svg = document.querySelector('svg');
6     svg.setAttribute('width', pan_pandef_res.clientWidth-30);
7     svg.setAttribute('height', pan_pandef_res.clientHeight-82);
8 }
```

Здесь в переменную *pan_pandef_res* записывается содержимое объекта с классом *.panel.panel-default.resizable*, а в переменную *svg* записывается содержимое svg-контейнера (поля с изображением графа). После этого в свойство высоты и ширины svg-контейнера записывается урезанные высота и ширина родительского объекта *pan_pandef_res* соответственно.

Также, были добавлены всплывающие подсказки при наведении указателя на основные кнопки управления (рис. 3).

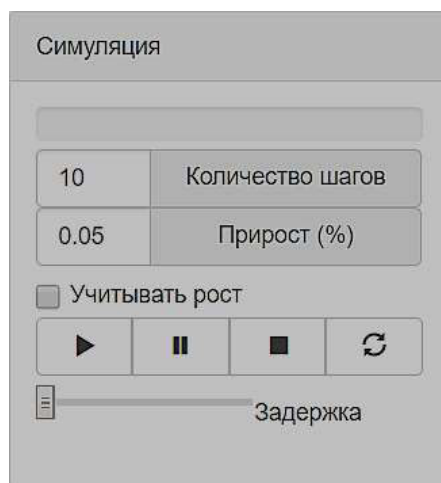


Рисунок 3 – Подпункт «Симуляция»

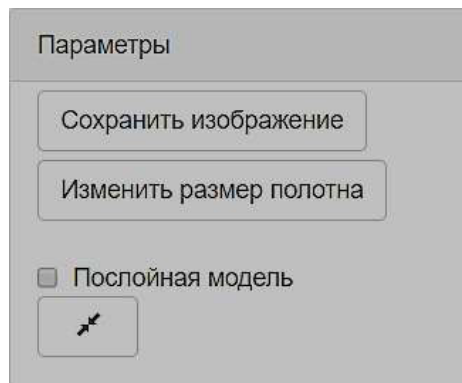


Рисунок 4 – Подпункт «Параметры»

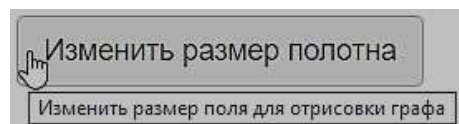


Рисунок 5 – Подписи для основных кнопок управления

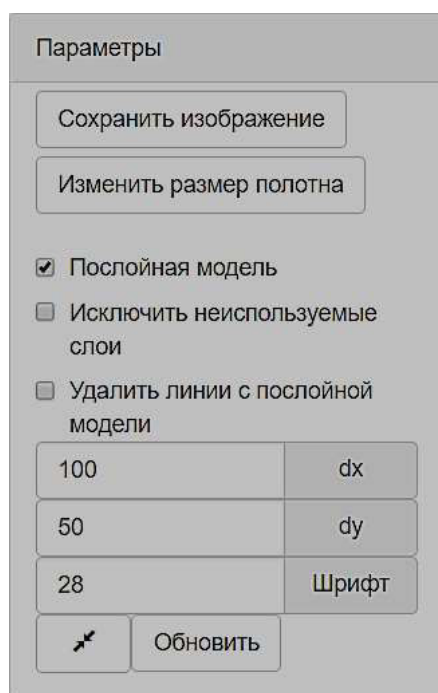


Рисунок 6 – Подпункт «Параметры» для послойной модели

При включении послойной модели флажком «Послойная модель» появляются дополнительные параметры. Здесь добавлен флажок «Удалить линии с послойной модели», который позволяет выключить отображение вспомогательных линий, показывающих слои в послойной модели, с помощью вызова функции *deleteCoralLines()*, в параметрах которой передается коэффициент прозрачности линий.

Данная функция имеет следующий вид:

```
1 function deleteCoralLines(val)
2 {
3   Element.prototype.SetAt = function(name, value)
4   {
5     this.parentElement.setAttribute(name, value);
6   }
7   NodeList.prototype.SetAt = HTMLCollection.prototype.SetAt = function(name, value) {
8     for(var i = this.length - 1; i >= 0; i--)
9     {
10      if(this[i] && this[i].parentElement)
11        this[i].parentElement.setAttribute(name, value);
12    }
13  }
14  document.querySelectorAll('[stroke=coral]').SetAt("stroke-opacity", val);
15  };
16
```

Здесь на строках 3-14 создается прототип функции установки атрибутов для объектов, в параметры которой передается имя атрибута и его значение. Это сделано для того, чтобы вызывать одну функцию сразу для всех объектов.

После чего на строке 15 вызывается метод выбора всех объектов, в которых атрибут *stroke* имеет свойство *coral*, и уже для всех выбранных объектов вызывается новосозданная функция установки атрибутов, где в атрибут прозрачности *stroke-opacity* передается определенное значение (1 – прозрачно, нет цвета; 0 – непрозрачно, имеет цвет).

На рисунке 7 представлена послойная модель с включенными вспомогательными линиями, а на рисунке 8 – без них.

Так как, зачастую, укладка графа и эпидемический процесс занимает большое количество времени, в программу были добавлены всплывающие подсказки, изображенные на рисунке 9. Они появляются после успешного обновления укладки графа и при окончании эпидемического процесса. Помимо этих условий, они могут быть в дальнейшем внедрены и для других событий, о которых следует информировать пользователя. Данные уведомления появляются даже тогда, когда окно с программой свернуто.

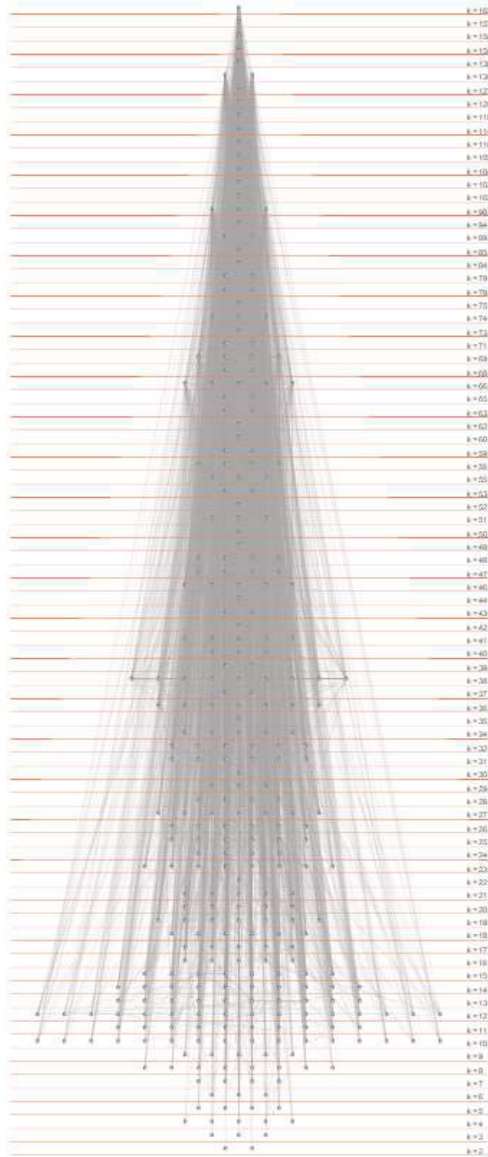


Рисунок 7 – Начальное представление послойной модели

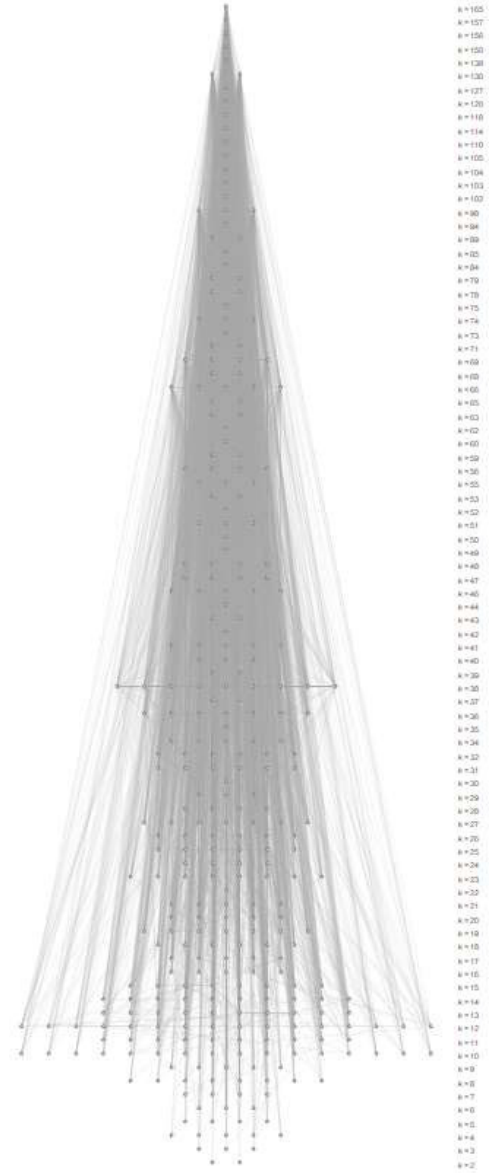


Рисунок 8 – Послойная модель после удаления вспомогательных линий-слоев

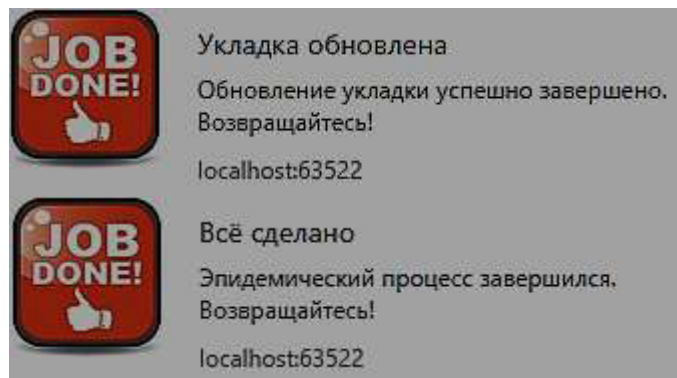


Рисунок 9 – Пример всплывающих уведомлений

Ниже представлен код обработки уведомлений.

```
1 function sendNotification(title, options)
2 {
3     if (!("Notification" in window)) {
4         alert(
5             'Ваш браузер не поддерживает HTML Notifications, его необходимо обновить.');
```

```
6     }
7     else if (Notification.permission === "granted") {
8         var notification = new Notification(title, options);
9         function clickFunc()
10        {
11            //alert('Вы были перемещены в программу!');
12            notification.close.bind(notification);
13        }
14        notification.onclick = clickFunc;
15        setTimeout(notification.close.bind(notification), 4000);
16    }
17    else if (Notification.permission !== 'denied') {
18        Notification.requestPermission(function (permission) {
19            if (permission === "granted") {
20                var notification = new Notification(title, options);
21            }
22            else { alert('Вы запретили показывать уведомления'); }
23        });
24    }
25    else { }
26 }
```

Здесь в параметры функции передаются заголовок уведомления и дополнительный текст. Далее происходит проверка, поддерживает ли используемый браузер HTML5 Notification. Если поддержки нет, то выдается окно с предупреждением, иначе проверяется наличие прав на отправку уведомлений. Если права есть (granted), то создается новое уведомление с заданными параметрами, а при клике на уведомлении выполняется обработчик функции clickFunc. На строке 15 устанавливается таймер закрытия уведомления через 4 секунды. Если прав на отправку уведомлений нет, происходит попытка их получения. При успешном получении создается новое уведомление с заданными параметрами, а при отказе выдается окно с предупреждением. На 25 строке ничего не выполняется, так как пользователь ранее отклонил запрос на показ уведомлений. В этом месте можно выполнить определенный код,

например, для отправки нового запроса, но нужно уважать решение пользователя, поэтому ничего не происходит.

Функция *notifyMe()* для отправки уведомлений имеет следующий вид:

```
1 this.notifyMe = function(titleText, bodyText)
2 {
3     sendNotification(titleText,
4                       { tag: 'ache-mail',
5                         body: bodyText,
6                         icon: '/job_done.jpg',
7                         dir: 'auto' });
8 }
```

Параметр *titleText* содержит заголовок уведомления, *tag* – тип уведомления, *body* – основное содержание уведомления, *icon* – изображение для уведомления, а *dir* – выравнивание содержимого уведомления.

Непосредственно в программе уведомление вызывается следующим кодом, например, в случае события обновления укладки:

```
1 _this.notifyMe('Укладка обновлена',
2 'Обновление укладки успешно завершено. Возвращайтесь!');
```

Вышеописанные изменения призваны повысить удобство пользования разрабатываемой программой для конечного пользователя.

На рисунках 10 и 11 представлены изменения структуры графа на примере социальной сети SoundCloud с учетом динамики ее развития.

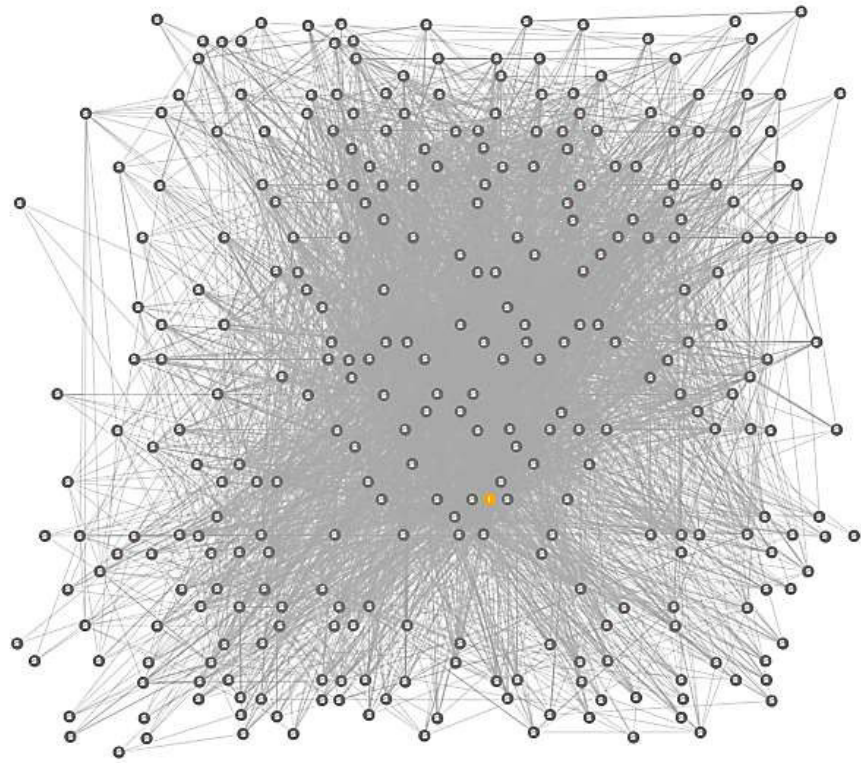


Рисунок 10 – Граф в начале эпидемического процесса



Рисунок 11 – Граф в конце эпидемического процесса при учете динамического развития сети

В качестве входных параметров была взята сеть с 309 вершинами и 6192 ребрами, установлены 30 шагов эпидемии и введен коэффициент прироста, равный 5% для наглядности. После окончания эпидемического процесса сеть выросла до 1302 вершин и 8380 ребер, что видно на графиках (рис. 12).

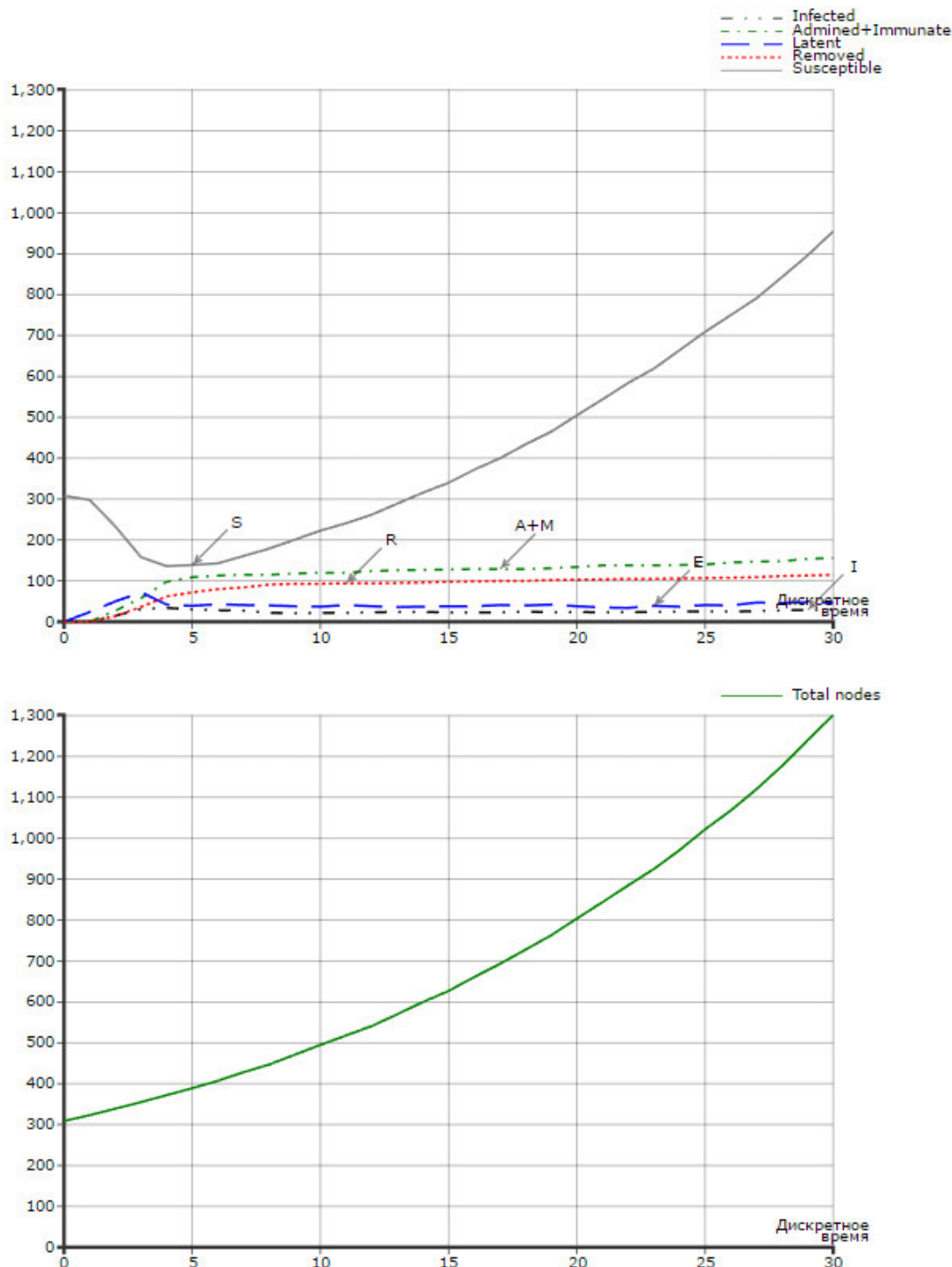


Рисунок 12 – График изменения общего количества вершин при учете динамического развития во время эпидемического процесса

Принципиальным преимуществом настоящего программного комплекса является его опора на дискретные модели, которые, в отличие от традиционных моделей аналогового характера, позволяют прогнозировать эпидемический процесс:

- на основе реальной статистики топологии и силы связей пользователей сети через удельный трафик оценивать взвешенно риски и шансы диффузии контента;
- для произвольных количества и расположения в сети источников деструктивного контента пошагово определять оптимальные параметры информационных диффузий;
- при коррекции параметров по ходу моделирования, управляя тем самым эпистойкостью сети;
- в условиях возможного репостинга контента, повышающего вероятности перехода вершин из одного эпидемического состояния в другое, которое также могут даваться, исходя из специфики конструкции и тематики контента;
- при столкновении конкурирующих контентов с сетью, что имеет место быть в ходе информационного противоборства, характерного для современных социальных сетей;
- при динамическом росте, что происходит практически во всех сетях, которые так или иначе развиваются.

В заключении следует заметить, что предлагаемый программный комплекс пригоден для моделирования не только социальных сетей. Определенные режимы позволяют задать для исследования сеть произвольной конфигурации: однородные, пуассоновские, безмасштабные и др. Это дает возможность анализировать сети корпоративные, сети критической инфраструктуры и т.п. в условиях возникновения в них эпидемических процессов. Этот факт существенно расширяет пространство практического применения программно-технического комплекса «Безопасный Интернет».

6. ПАТЕНТОСПОСОБНОСТЬ

6.1 НАЛИЧИЕ ПАТЕНТА, ЗАЯВКИ НА ТЕХНИЧЕСКОЕ РЕШЕНИЕ, ПЛАНА ДЕЙСТВИЙ ПО ЗАЩИТЕ ПРАВ НА ИНТЕЛЛЕКТУАЛЬНУЮ СОБСТВЕННОСТЬ

Подана и зарегистрирована заявка на изобретение в ОЦНИТ ВГТУ – "Комплекс прикладных программ для риск-анализа процессов распространения деструктивного контента в неоднородных сетевых структурах. Регистрационный № .02068083.04137-01.

Получено свидетельство РОСПАТЕНТа о государственной регистрации программы для ЭВМ №2016662015. Netepidemic, от 09.01.17.

6.2 ПАТЕНТНАЯ ЧИСТОТА, КАЧЕСТВО ПАТЕНТНОГО ПОИСКА (ПРОВЕРКА НОВИЗНЫ И НАЛИЧИЯ БЛИЖАЙШИХ АНАЛОГОВ)

Ссылки на наиболее близкие к создаваемому программному комплексу зарубежные патенты, обладателем которых являются третьи лица:

Патенты:

1. Анализ рисков в социальной сети

a. Номер: 8799028;

b. Страна: США;

c. Описание: Измененный модуль социальной сети, связанный с оставшейся ее частью, может создать свою социальную сеть для личности, группы и/или организации. После того модуль может использовать социальную сеть для определения риска, связанного с идентификацией представителей социальной сети. Полученный риск может быть использован для определения рейтинга подтверждения участников сети, а также различных мер центральности участников.

2. Измерение рисков на основе информации о социальной сети

a. Номер: 2014145431;

b. Страна: Мировая организация интеллектуальной собственности;

с. Описание: Представлены инструменты, стратегии и техники оценки личности для различных обществ, чтобы защитить индивидуальных потребителей, бизнес-решения и другие организации от кражи личности и мошенничества. Риски, связанные с конкретными обществами могут быть определены на основе данных социальных сетей, профессиональной сети и любых других сетей среди различных источников информации.

3. Получение обратной связи риска безопасности от связанного контакта на основе системы действий и поведения пользователя

a. Номер: 8712921;

b. Страна: США;

с. Описание: Представлен подход на основе получения отклика риска из социальной сети. Отклики пользовательская система получает с каждой операцией получения пакетов от контактов социальной сети. Отклики анализируются, и по результатам анализа определяются рискованные взаимодействия в сети. Пользователь выполняет меры предупреждения риска. В некоторых вариантах данные меры отсылаются контактам.

4. Система и методика классификации явлений заражения, распространяющихся в сети

a. Номер: 20130232263;

b. Страна: США;

с. Описание: Классификация явлений заражения может быть основана на количестве островеершинностей, заражении, заражении последующего использования, заражении по времени и явлениям дисперсии, связанным с взаимодействием с заразительным феноменом.

7. ЗНАЧИМОСТЬ ПРОЕКТА

7.1 ВЛИЯНИЕ НА РОСТ УРОВНЯ И ПОВЫШЕНИЕ КАЧЕСТВА ЖИЗНИ НАСЕЛЕНИЯ

Сравнительно недавно наступила новая ступень в развитии обмена информацией, которая базируется на интенсивном внедрении современных информационных технологий, на широком распространении локальных, корпоративных и глобальных сетей во всех сферах жизни цивилизованного государства, она, также, формирует новые возможности и качество информационного обмена. В этом есть и отрицательная сторона. В информационных сетях может распространяться контент практически любого характера, в том числе и деструктивного. Согласно Доктрине информационной безопасности, утвержденной Указом Президента Российской Федерации от 5 декабря 2016 г. №646, данная проблема особенно остро поднимается в последнее время из-за увеличения количества различных инцидентов, так или иначе, связанных с распространением деструктивного контента в информационных сетях. В качестве примера возросшего информационно-психологического влияния на людей, а в частности подростков, можно привести игру “Синий кит”, информация о которой начала активно появляться с мая 2016 года.

Таким образом, онлайн-социальные сети, которые обладают огромной популярностью, постепенно становятся основным инструментом информационно-психологического воздействия на общество.

Исходя из вышенаписанного, можно выделить, что актуальность разработанного программного комплекса обусловлена следующими факторами:

1. Ростом популярности информационных социальных сетей и небрежного отношения людей к добавлению вредоносной информации в закладки, которая может быть получена при переходе по фишинговым ссылкам или от "засланных" пользователей сервиса;

2. Ростом скорости развития технологий, а, следовательно, и ростом мощностей деструктивных воздействий на информационные сети;
3. Присутствием в информационных сетях огромного количества вредоносного контента, который имеет деструктивный характер;
4. Ограниченной осведомленностью людей об определении полезной и ценной информации, которая используется в рассматриваемых сервисах;
5. Относительно слабой защищенностью социальных сетей от разного вида атак и необходимостью обеспечения пользователей безопасностью при нахождении в данных сетях;
6. Потребностью в создании определенной системы, позволяющей управлять возникающими рисками и устранять их в рассматриваемых сервисах.

Таким образом, в данной области жизненно необходим комплекс научно-методического обеспечения, которое позволит управлять информационными рисками на основе данных о вероятном ущербе при возникновении различных угроз, для повышения общего уровня защищенности различных информационных сетей и их пользователей.

7.2 ВЛИЯНИЕ НА БЕЗОПАСНОСТЬ НАСЕЛЕНИЯ

Онлайновые социальные сети, обладают огромной популярностью, постепенно становятся основным инструментом информационно-психологического воздействия на общество. Таким образом, в данной области необходимо создание комплексного научно-методического обеспечения, которое позволит управлять информационными рисками на основе данных о вероятном ущербе при возникновении различных угроз, для повышения общего уровня защищенности различных информационных сетей и их пользователей. Повышение защищенности систем, которые представляют из себя информационные сети, и процессов, которые в них протекают, является одним из приоритетных направлений исследования и остается актуальной на протяжении довольно большого временного периода.

7.3 СОЗДАНИЕ КОНКУРЕНТОСПОСОБНОГО, ВЫСОКОТЕХНОЛОГИЧНОГО ПРОМЫШЛЕННОГО КОМПЛЕКСА В РЕГИОНЕ

В пределах нашего региона отсутствуют аналоги по данной тематике, а на рынке приложений продукт выигрывает тем, что он русскоязычный и имеет достаточно простой интерфейс по сравнению с ближайшими аналогами.

7.4 ФОРМИРОВАНИЕ УСЛОВИЙ ДЛЯ ИСПОЛЬЗОВАНИЯ НАУЧНО- ТЕХНИЧЕСКОГО ПОТЕНЦИАЛА ВОРОНЕЖСКОЙ ОБЛАСТИ В ЦЕЛЯХ ПОВЫШЕНИЯ КОНКУРЕНТОСПОСОБНОСТИ ПРОМЫШЛЕННОСТИ

Программный комплекс направлен на повышение инвестиционной привлекательности Воронежской области, формирование условий для мобилизации внутренних и увеличения притока внешних инвестиционных ресурсов и новых технологий в экономику Воронежской области. Проект разработан в соответствии с одним из основных направлений ФГБОУ ВПО «Воронежский государственный технический университет» «Управление информационными рисками и обеспечение безопасности инфокоммуникационных технологий» на базе Воронежского научно-образовательного центра управления информационными рисками. в рамках проводимой региональной программы «Безопасный интернет».