МЕМОРАНДУМ

о ПРОТИВОДЕЙСТВИи РАСПРОСТРАНЕНИЮ ВРЕДОНОСНЫХ ПРОГРАММ (ВИРУСОВ) И

НЕСАНКЦИОНИРОВАННЫХ РЕКЛАМНЫХ РАССЫЛОК (СПАМА)

**г. Москва, 2003 г.**

Содержание

**ВВЕДЕНИЕ**…….. 3

**ГЛАВА 1. НЕГАТИВНОЕ ВЛИЯНИЕ ВРЕДОНОСНЫХ**

**ПРОГРАММ И СПАМА** 5

1.1. Государственные инфокоммуникационные системы 7

1.2. Инфокоммуникационные системы коммерческих

и некоммерческих организаций 7

1.3. Персональные инфокоммуникационные системы 8

**ГЛАВА 2. ЗАДАЧИ ЗАЩИТЫ ОТ ВРЕДОНОСНЫХ ПРОГРАММ**

**И СПАМА** 9

2.1. Совершенствование нормативной базы 9

2.2. Разработка Политики Безопасности 10

2.3. Проведение образовательной работы 11

2.4. Задачи разработчиков технических средств ..12

2.5. Задачи системных интеграторов 12

2.6. Задачи операторов связи 13

2.7. Задачи органов государственной власти 14

**ЗАКЛЮЧЕНИЕ.** 15

# Введение

Настоящий документ разработан общественно-государственным объединением «Ассоциация Документальной Электросвязи» в соответствии с поручением Министра Российской Федерации по связи и информатизации. В разработке и обсуждении документа принимали участие: Аветиков Сергей Юрьевич (СЦС «Совинтел»), Антимонов Сергей Григорьевич (ДиалогНаука), Ашманов Игорь Станиславович (Ашманов и Партнеры), Баранов Сергей Геннадьевич (ВГТРК), Брюханов Андрей Анатольевич (Инфосистемы Джет), Быканов Александр Владимирович (Ростелеком), Ваньков Вадим Валерьевич (МТУ-Интел), Ганев Михаил Игоревич (РосНИИРОС), Диденко Петр Владимирович (Зенон Н.С.П.), Желонкина Татьяна Германовна (Mail.ru), Засурский Иван Иванович (Rambler), Кадер Михаил Юрьевич (Сиско Системс), Кашинский Сергей Иванович (Инфосистемы Джет), Коваленко Николай Павлович (ЦНИИС), Колмановская Елена Савельевна (Яндекс), Кондаков Гарри Игоревич (Лаборатория Касперского), Кононов Александр Анатольевич (ИСА РАН), Корешков Юрий Петрович (Минсвязи России), Кремер Аркадий Соломонович (Исполком АДЭ), Курносов Иван Николаевич (Минсвязи России), Линде Сергей Юрьевич (РосНИИРОС), Лозинский Дмитрий Николаевич (ДиалогНаука), Муругов Сергей Михайлович (РосНИИРОС), Новиков Николай Александрович (Минсвязи России), Першов Александр Николаевич (Минсвязи России), Соболев Дмитрий Владимирович (Компания ТрансТелеКом), Сундуков Александр Георгиевич (Минсвязи России), Тимошин Владимир Николаевич (Лаборатория Касперского), Трифаленков Илья Анатольевич (Инфосистемы Джет), Федотов Николай Николаевич (РТКомм.РУ), Фролов Александр Вячеславович (Служба Data Recovery.ru), Шаров Борис Александрович (ДиалогНаука), Якушев Михаил Владимирович (Майкрософт).

Меморандум предполагает объединение вокруг Минсвязи России всех, кто заинтересован в создании мощного барьера на пути распространения вредоносных программ и спама.

В первой главе рассматривается негативное влияние вредоносных программ и спама на государственные, коммерческие, некоммерческие и персональные инфокоммуникационные системы. Дается классификация различных категорий пользователей: государственные организации, коммерческие и некоммерческие организации, частные пользователи. Для каждой категории пользователей рассматриваются особенности защиты от вредоносных программ и спама.

Во второй главе определены первоочередные меры по противодействию распространению вредоносных программ и спама.

В заключительной части документа приводятся выводы и рекомендации.

**Основные термины и определения, используемые в данном документе.**

**Вирусная атака —** намеренное распространение вредоносных программ (в частности, компьютерных вирусов), предпринимаемое с целью вывести инфокоммуникационную систему из строя, получить несанкционированный доступ к системе, изменить хранящуюся в системе информацию или выполнить другое вредоносное действие.

**Вредоносная программа** — программа (часть программы), которая заведомо приводит к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети.

**Компьютерный вирус** — программа (некоторая совокупность выполняемого кода/инструкций), способная создавать свои копии, не обязательно полностью  
совпадающие с оригиналом, и внедрять их в различные объекты/ресурсы  
компьютерных систем, сетей и т.д. без ведома пользователя. Такая программа является заведомо вредоносной.   
**Спам —** сообщения электронной почты рекламного или иного характера, рассылаемые адресатам, которые не выразили в явной или неявной форме желания получать такие сообщения, либо выразили нежелание их получать. Основными характеристиками спама являются, как правило, массовость рассылки и анонимность рекламораспространителя.

# Глава 1. Негативное влияние вредоносных программ и спама

На начальном этапе развития сетевых технологий ущерб от вирусных и других типов компьютерных атак был незначителен вследствие несущественной зависимости российской экономики от информационных технологий. В настоящее время в условиях постоянно растущего числа атак, создания механизмов по их автоматизации, а также значительной зависимости граждан, бизнеса и органов государственной власти от электронных средств доступа и обмена информацией, ущерб от реализации атак на инфокоммуникационные системы исчисляется огромными суммами.

По мере развития и внедрения интернет-технологий в инфокоммуникационные системы сеть Интернет, а также интрасети компаний и организаций начинают активно использоваться для выполнения деструктивных действий. Проникая в сеть компании или организации, вредоносная программа может выполнить разнообразные деструктивные действия: от уничтожения и хищения информации до полного блокирования работы системы. Не меньший вред способна нанести и несанкционированная рассылка сообщений электронной почты (спам), рассматриваемая как один из видов атак через Интернет.

По данным компании Computer Economics в мировом масштабе за прошлый год ущерб от вирусов и других вредоносных программ составил $14.5 млрд. Ситуация с распространением компьютерных вирусов постоянно ухудшается. По данным компании ICSA Labs, в период с 1996 по 2002 годы количество инфицированных компьютеров увеличилось с 1% до 10.5%. При этом затраты на восстановление информации выросли за последний год почти в два раза. Согласно оценкам компании Яндекс, около 60% писем представляют собой спам. На получение и чтение спама пользователи Интернета тратят большое количество времени и денег. Согласно оценкам интернет-холдинга Rambler, получение спама приводит к убыткам пользователей российского Интернета, превышающим 200 млн. долл. в год. Только частные интернет-пользователи России ежегодно платят совокупный «налог на спам» порядка 120 млн. долл. Это в шесть раз больше, чем было выделено в 2002 г. на программу «Электронная Россия». В мире отчетливо прослеживается тенденция к увеличению процентного содержания спама. И если в 2001 г. спам занимал лишь 8% всего трафика электронной почты и обошелся пользователям Интернета во всем мире в 10 млрд. евро, то в 2002 г. впервые за всю историю электронной почты доля спама в общем трафике сообщений превысила 40%. К 2007 г., по прогнозу компании Radicati Group, спам составит 70% от всего объема электронной почты. По данным западных экспертов (CNews Analytics), количество хакерских атак против России значительно выросло в ноябре 2002 года, что поставило нашу страну на 10 строчку наиболее атакуемых стран в этом месяце, хотя до и после этого Россия ни разу не появлялась даже в двадцатке наиболее атакуемых стран 2002 года. Количество компьютерных атак с начала 2003 года по 16 апреля 2003 года составило 143. На начало апреля наметилась тенденция к снижению количества проведенных в отношении российских инфокоммуникационных систем атак. Однако летом следует ожидать небольшого роста числа нарушений безопасности, который связан с сезоном отпусков и, как следствие, снижением внимания организаций к обеспечению своей информационной безопасности.

Острой проблемой в настоящее время является низкий уровень обеспечения информационной безопасности большинства систем, подключенных к глобальной сети. Среди факторов, напрямую влияющих на уровень безопасности инфокоммуникационных систем, особое место занимает коммерческое программное обеспечение (ПО), для которого большое количество опций и быстрый вывод на рынок зачастую имеет большее значение, чем его безопасность. Разработчиками, взломщиками и независимыми исследовательскими группами постоянно выявляются ошибки в таком ПО. Распространение коммерческих продуктов в глобальном масштабе означает, что как только обнаружена уязвимость, взломщик может многократно использовать ее на сотнях тысяч или даже миллионах систем, на которых установлен недоработанный в плане безопасности продукт. Недостаточный уровень подготовки пользователей зачастую приводит к тому, что они не могут самостоятельно проводить обновления ПО, устраняющие уязвимости в системе. В результате система может легко подвергнуться атакам со стороны злоумышленников и в последствии использоваться в качестве стартовых позиций для реализации атак на более защищенные системы или  использоваться для маскирования маршрута атаки.

Отдельно следует отметить повсеместное использование организациями и персональными пользователями не лицензированного ПО. Используя такое программное обеспечение, пользователи ограничивают себя «устаревшей» защитой от давно обнаруженных вирусов. Отсутствие оперативного обновления вирусной базы и квалифицированной технической поддержки, предоставляемой официальным покупателям, отрицательно сказывается на безопасности инфокоммуникаций.

С учётом типа используемой информации, объема внешних инфокоммуникационных связей и степени регулирования можно выделить три основных типа инфокоммуникационных систем, в разной степени подверженных негативному влиянию вредоносных программ и спама: государственные, системы коммерческих и некоммерческих организаций, индивидуальные.

## Государственные инфокоммуникационные системы

Деятельность государственных организаций оказывает влияние на все общество, и объективно они являются более открытыми, чем коммерческие. В рамках государственных программ, таких, например, как «Электронная Россия», предполагается реализация электронного взаимодействия граждан с государственными структурами. Это делает инфокоммуникации государственных органов особенно уязвимыми для вредоносных программ.

Поражение государственных инфокоммуникационных систем вредоносными программами может затронуть интересы всей страны.

Спам также способен нанести государству ощутимый ущерб, так как он приводит к непроизводительным расходам на оплату трафика и времени подключения к Интернету, а также к потерям рабочего времени государственных служащих.

Другой важный аспект связан с тем, что в органах государственной власти отсутствуют дублирующие структуры. У потребителя нет возможности выбрать другую организацию в случае, если информационная система нужной ему государственной организации перегружена спамом или выйдет из строя в результате воздействия вредоносных программ.

Объективно государство обладает большими возможностями регулирования своей работы. Это создает хорошие предпосылки для проведения административно-технических мероприятий, обеспечивающих защиту государственных инфокоммуникационных систем. В то же время многие государственные организации не обладают необходимыми ресурсами защиты. В таких организациях на рабочих местах и в серверных комплексах используются программные продукты, не обладающие устойчивостью к воздействию вирусных атак. Средства защиты от спама также редко используются государственными организациями.

С учетом важности и масштабности государственных инфокоммуникационных систем задача обеспечения их информационной безопасности имеет особое значение.

## Инфокоммуникационные системы коммерческих и некоммерческих организаций

Информация, хранящаяся в инфокоммуникационных системах коммерческих и некоммерческих организаций, имеет ценность только для данных организаций, их партнеров и клиентов. Поэтому масштабы ущерба от ее потери или искажения будут в целом меньше возможного ущерба от потери или искажения информации государственных организаций.

Тем не менее, по масштабам возможного ущерба, связанного с воздействием вредоносных программ и спама, крупные коммерческие и некоммерческие организации могут сравниваться с государственными структурами. Как правило, организации разрабатывают и реализуют собственные политики информационной безопасности.

## Персональные инфокоммуникационные системы

Защита персональных инфокоммуникационных систем (например, компьютеров) от вредоносных программ и спама является прерогативой владельцев этих систем. Ущерб от повреждения информации, хранящейся в персональной системе, как правило, относительно невелик и затрагивает только владельца этой системы. Для персональных информационных систем характерна закрытость и слабая регулируемость.

Сотрудники государственных или негосударственных организаций, решающие служебные вопросы дома на персональной системе, могут неумышленно сделать свою систему стартовой для реализации атак на служебную инфокоммуникационную систему, либо способствовать утечке служебной информации, либо непреднамеренно принести на рабочее место вредоносную программу с домашнего компьютера. При этом возможно массовое распространение вредоносных программ и возникновение вирусных эпидемий.

# Глава 2. Задачи защиты от вредоносных программ и спама

Для эффективного противодействия распространению вредоносных программ и спама необходимо принятие комплексных мер на различных уровнях. Решение данной задачи невозможно без участия всех заинтересованных сторон. В процесс решения поставленной задачи необходимо вовлечь:

* разработчиков программного и аппаратного обеспечения;
* системных интеграторов;
* операторов связи;
* исполнительные и законодательные органы государственной власти.

Следует учитывать тот факт, что никакие меры не смогут гарантировать достижения полной защиты. Речь может идти только о минимизации рисков, а не о полном их исключении.

## 2.1. Совершенствование нормативной базы

Одним из направлений совершенствования нормативной базы применительно к вредоносным программам и спаму является надлежащее обеспечение построения системы информационной безопасности при использовании сертифицированных и лицензионных технических средств с последующей аттестацией системы.

Несмотря на значительное количество действующих нормативных актов в области защиты информации, существует разрыв между реальным уровнем информационных и коммуникационных технологий и нормативным обеспечением, регулирующим их проектирование, внедрение и эксплуатацию. Необходимо, в частности, выпустить документ по терминам и определениям в области вредоносных программ и спама, исключающий неоднозначное толкование соответствующих понятий. Представляется целесообразным проработать вопрос о нормативном закреплении ответственности государственных служащих и работников негосударственных организаций за соблюдение политики безопасности в организациях (в частности, за действия, способные привести к распространению вирусов или снижению устойчивости инфокоммуникационной системы к атакам).

В нормативно-техническом плане необходима разработка набора профилей защиты от вредоносных программ, в соответствии со стандартом ГОСТ/ИСО МЭК 15408.

В настоящее время нет необходимости в принятии отдельного законодательного акта, предметом регулирования в котором был бы спам; пока было бы достаточным внесение изменений и дополнений в действующие федеральные законы и нормативно-правовые акты иного уровня.

Федеральный закон «О рекламе» необходимо дополнить статьёй о распространении рекламы с использованием электронных средств (включая компьютерные сети и средства связи), установив, что к такому распространению применяется общий режим регулирования рекламной деятельности с особенностями, вытекающими из специфики используемых технических средств.

Кодекс об административных правонарушениях необходимо дополнить статьёй об административной ответственности за распространение незапрошенных электронных и почтовых сообщений рекламного и иного характера.

Федеральный закон «О почтовой связи» необходимо дополнить положением о порядке доставки почтовой корреспонденции в почтовые ящики, абоненты которых явно выразили нежелание получать сообщения рекламного характера. Речь идет не о том, чтобы запретить вообще получать письма и газеты, а том, чтобы, во-первых, все почтовые сообщения проходили бы через почтовые отделения (т.е. были бы запечатаны и с наклеенными знаками почтовой оплаты), и, во-вторых, сообщения, отмеченные как «рекламные», не доставлялись бы в почтовые ящики с наклейками типа «рекламу не опускать!».

## 2.2. Разработка Политики Безопасности

Под политикой безопасности понимается совокупность документированных управленческих решений, направленных на обеспечение информационной безопасности. Политика безопасности определяет стратегию организации в области информационной безопасности, а также ту меру внимания и количество ресурсов, которые руководство организации считает целесообразным выделить как критичную.

Политика безопасности должна включать в себя комплексные решения, охватывающие все аспекты использования инфокоммуникационных систем. В документ, характеризующий политику безопасности организации, представляется целесообразным включать следующие разделы:

* вводный, определяющий роль и место обеспечения информационной безопасности в инфокоммуникационной системе;
* организационный, содержащий описание подразделений, комиссий, групп и т.д., отвечающих за работы в области обеспечения информационной безопасности;
* классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
* штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организацию обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
* раздел, освещающий вопросы физической защиты оборудования инфокоммуникаций;
* управляющий раздел, описывающий подход к управлению техническими средствами;
* раздел, описывающий правила разграничения доступа к информационным ресурсам;
* раздел, характеризующий порядок разработки и сопровождения автоматизированных информационных систем;
* раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
* юридический раздел, подтверждающий соответствие политики безопасности действующему законодательству и внутренней нормативно-распорядительной документации.

Созданная однажды политика безопасности не должна рассматриваться как догма. Ее необходимо постоянно пересматривать и корректировать по мере развития инфокоммуникационных технологий, а также по мере появления новых угроз.

## 2.3. Проведение образовательной работы

Отсутствие необходимых знаний в области защиты от вредоносных программ и спама является источником возникновения проблем с обеспечением информационной безопасности.

На первом этапе для налаживания образовательной работы, направленной на противодействие угрозам информационной безопасности, можно предложить следующие меры:

* разработка кратких брошюр и методических указаний с рекомендациями по информационной защите для руководителей различного звена, администраторов информационных систем, пользователей офисных и домашних компьютеров;
* разработка руководств, отражающих все изученные аспекты информационной защиты с практической точки зрения, а также постоянное дополнение и обновление таких руководств;
* разработка учебных программ и методических материалов для проведения учебных занятий в высших и специальных учебных заведениях, на курсах повышения квалификации специалистов, а также проведение таких занятий;
* создание и постоянное обновление информационных ресурсов Интернета, посвященных защите от вредоносных программ и атак злоумышленников, списков рассылок новостей, конференций и других аналогичных ресурсов;
* создание пособий для школьников, посвященных основам информационной безопасности;
* создание постоянно действующих форумов, в рамках которых группы специалистов могли бы обмениваться опытом противодействия угрозам информационной безопасности;
* проработка вопросов создания единой национальной системы информирования государственных, коммерческих, некоммерческих организаций, а также индивидуальных пользователей компьютеров о возникновении новых угроз информационной безопасности.

Образовательная работа должна вестись широким фронтом и на постоянной основе, так как только в этом случае можно обеспечить адекватное реагирование на появление новых угроз информационной безопасности.

## 2.4. Задачи разработчиков технических средств

В рамках решения задач по защите от вредоносных программ и спама разработчикам технических средств необходимо:

* постоянно развивать средства защиты от вредоносных программ и спама, отслеживая современные тенденции в этой области;
* участвовать в формировании согласованного набора требований к средствам защиты от вредоносных программ и критериев их объективной проверки;
* обеспечивать возможность привлекательной финансовой схемы внедрения и сопровождения средств защиты от вредоносных программ и спама;
* оказывать всемерное содействие проведению просветительской работы, направленной на повышение квалификации технических специалистов и руководителей в области защиты от вредоносных программ и спама;
* принимать активное участие в нормотворческой деятельности, способствуя разработке действенных и непротиворечивых нормативных документов в области компьютерных технологий.

## 2.5. Задачи системных интеграторов

Системные интеграторы из набора отдельных средств защиты информации создают системы обеспечения информационной безопасности и осуществляют поддержку предложенных решений на стадии их эксплуатации. Задачами системных интеграторов являются:

* формирование наборов стандартизованных решений, обеспечивающих полноту и экономическую эффективность мер защиты информации в инфокоммуникационных системах;
* обеспечение внешнего мониторинга уровня защищенности инфокоммуникационных систем;
* формирование требований к качеству предоставляемых услуг с учетом применения средств защиты от вредоносных программ и спама;
* участие в формировании требований к производителям технических средств защиты с точки зрения реализации системы обеспечения информационной безопасности и ее сопровождения в процессе эксплуатации;
* участие в организации систем оповещения и предупреждения об угрозах, связанных с использованием вредоносных программ;
* участие в нормотворческой деятельности.

Перечисленные задачи определяют место системного интегратора как связующего звена между разработчиками технических средств защиты информации, операторами и пользователями инфокоммуникационных систем.

## 2.6. Задачи операторов связи

Основной средой распространения вредоносных программ и спама являются телекоммуникационные сети, объединяющие владельцев информационных систем и ресурсов, поэтому операторы связи должны быть активно вовлечены в процесс противодействия распространению вредоносных программ и спама.

Учитывая то обстоятельство, что операторы могут оказывать пользователям услуги одной службы электросвязи (телефонной, телеграфной, телематической, передачи данных и т.п.) или нескольких служб, включая все существующие их разновидности, должны различаться и предъявляемые к ним требования по противодействию распространению вредоносных программ и спама.

При этом следует отметить, что все без исключения операторы связи, должны быть заинтересованы в обеспечении надежной и безопасной передачи информации как основы своей деятельности, поэтому, должны располагать подготовленным штатом сотрудников и продуманными регламентами, в том числе по предотвращению распространения вредоносных программ и спама. Исходя из этого в качестве первоочередных задач, которые в состоянии решить вышеперечисленные группы  операторов следует определить:

* организацию службы реагирования на инциденты информационной безопасности (RFC2350, 3013). В случае невозможности организации полноценной службы, создание  почтовых учетных записей, определенных RFC2142, Abuse, Security и реагирование на корреспонденцию, приходящую на эти почтовые ящики;
* поддержание в актуальном состоянии собственных записей в базах данных RIPN, RIPE, ARIN и т.д.;
* взаимодействие с клиентами в случае инцидентов, связанных с распространением  вредоносных программам и спама;
* взаимодействие с государственными органами, ведущими противодействие распространению вредоносных программ и спама.

Первоочередные задачи всех групп операторов должны дополняться рекомендуемыми требованиями по:

* поддержанию защищенности собственных информационных ресурсов в актуальном состоянии, путем устранения обнаруженных уязвимостей;
* принятию участия в формировании требований к «доверительным участкам общедоступных сетей»;
* принятию участия в формировании требований к базовому уровню обеспечения безопасности оператора связи, введенному в проекте документа «Концепция информационной безопасности Сетей связи общего пользования Взаимоувязанной сети связи Российской Федерации»;
* разработке и внедрении услуг по:

-аудиту защищенности информационных ресурсов;

-формированию сегментов сети, с реализованными системами защиты от угроз информационной безопасности.

Внедрение подобных услуг создаст предпосылки для создания участков Российского Интернета, подключение к которым существенно снижает вероятность возникновения ущерба от вредоносных программ, спама и атак злоумышленников.

Для группы операторов, предоставляющих услуги информационных сервисов, рекомендуемые требования  по противодействию распространению вредоносных программ и спама должны быть расширены, путем  разработки и внедрения таких дополнительных услуг как:

* предоставление антивирусной защиты на почтовых и иных серверах;
* фильтрация трафика с целью блокирования распространения вредоносных программ и спама.

## 2.7. Задачи органов государственной власти

Основными задачами органов государственной власти, а также юристов, работающих в данной предметной области, являются:

* совершенствование нормативной базы в области противодействия распространению вредоносных программ и спама;
* привлечение к нормотворческой деятельности экспертов в области инфокоммуникационных технологий и систем обеспечения информационной безопасности;
* всемерная поддержка проведения образовательной работы;
* содействие в налаживании международного сотрудничества.

# Заключение

Задача противодействия распространению вредоносных программ и спама является весьма актуальной. Вредоносные программы и спам наносят ощутимый ущерб инфокоммуникационным системам, принадлежащим государственным, негосударственным организациям, а также частным лицам. При этом следует отметить, что в зависимости от специфики той или иной инфокоммуникационной системы, от ценности защищаемых ресурсов, меры противодействия могут быть более или менее строгими, но в любом случае следует избегать излишнего радикализма.

В рамках организационно-правовой деятельности необходимо разработать регламентирующие документы, направленные на защиту государственных, негосударственных и личных инфокоммуникационных систем. Предлагается создать рабочую группу под эгидой АДЭ для выполнения и координации дальнейших работ по подготовке проектов нормативных документов в этой области. В задачи этой группы могут входить:

* разработка набора профилей средств защиты информационных ресурсов от вредоносных программ;
* разработка мер, способствующих эффективному применению действующих нормативных документов;
* разработка требований к базовому уровню обеспечения информационной безопасности для операторов связи, включая проведение необходимых исследований в части противодействия распространению вредоносных программ и спама;
* разработка предложений по ответственности участников информационного обмена за  нарушение требований политики безопасности;
* разработка рекомендаций организациям и индивидуальным пользователям по противодействию распространению вредоносных программ и спама;
* разработка проектов нормативных документов, регламентирующих использование государственными органами ресурсов сети Интернет;
* подготовка предложений по созданию системы оперативного информирования государственных, негосударственных организаций и индивидуальных пользователей о возникновении угроз информационной безопасности.

В рамках технической деятельности представляется целесообразным на базе рабочей группы, подготовившей данный документ, образовать постоянно действующую рабочую группу для обсуждения и подготовки согласованных технических предложений (рекомендаций, стандартов) в области противодействия распространению вредоносных программ и спама.

В рамках образовательной деятельности необходимо организовать информирование пользователей о юридических средствах, технических и организационных ресурсах по борьбе с вредоносными программами и спамом. Целесообразно использовать для этих целей информационные ресурсы сети Интернет, средства массовой информации, другие информационные каналы.

В частности, в рамках образовательной деятельности необходимо предусмотреть:

* создание методических указаний, учебной литературы, инструкций, руководств, а также справочно-информационных ресурсов в Интернете с рекомендациями по информационной защите для руководителей различного звена, администраторов информационных систем, пользователей офисных и домашних компьютеров, преподавателей соответствующих дисциплин в высших и специальных учебных заведениях;
* разработку учебных программ и методических материалов для проведения учебных занятий в высших и специальных учебных заведениях и на курсах повышения квалификации специалистов и проведение таких занятий;
* обеспечение работы постоянно действующих форумов по обмену опытом противодействия угрозам компьютерной безопасности.

Решение задачи противодействия распространению вредоносных программ и спама возможно лишь совместными усилиями всех заинтересованных участников инфокоммуникационного рынка и при комплексном рассмотрении организационно-правовых, технических и образовательных вопросов.

Для эффективного противодействия распространению вирусов и спама необходимо международное сотрудничество.