А.В. Линьков, М.Е. Гордеева

АНОНИМНОСТЬ И ИНТЕРНЕТ

(Самарский государственный университет)

Современная жизнь невозможна без использования информационных технологий. Одной из таких технологий является Интернет, который прочно вошел в современную жизнь. В некоторых ситуациях, пользователь желает остаться анонимным, с целью защиты личных данных, например, о своем местоположении, паспортных данных, состоянии банковского счета и тому подобном. Под *анонимностью* можно понимать недоступность вышеперечисленных данных для обеспечения личного комфорта и безопасности пользователя сети Интернет. Анонимность пользователя в сети в общем случае можно рассматривать через призму понятий информационной безопасности. В частности, проблемы анонимности имеют отношение к безопасности в сети. В последнее время информационной безопасности личности и ее взаимосвязи с информационной безопасностью государства в постиндустриальном обществе [1, 2] уделяется большое внимание. Проблема анонимности тесно связана с проблемами свободы слова и печати, ограничения распространения информации ограниченного доступа, защиты информации и обеспечения безопасности информационных процессов в глобальных телекоммуникационных сетях, которые сейчас имеют не только теоретическое но большое практическое значение.

Проблемы анонимности в сети можно и нужно подвергать анализу с нескольких направлений. Во-первых, можно выделить правовую и техническую составляющие. Во-вторых, при анализе проблемы с выделенных точек зрения, анонимность в интернете требует учёта непосредственных интересов пользователя, государства и злоумышленника. В данной статье анализируется правовая составляющая выделенной проблемы.

При исследовании механизмов анонимности в сети Интернет необходимо провести анализ основных законов и нормативно-правовых актов, регулирующих отношения между гражданами РФ, в том числе и в сети Интернет, поскольку эти нормы являются основой для правового регулирования взаимодействия пользователей в Интернете (по крайней мере, в Рунете).

Конституция РФ предусматривают основные права и правомочия пользователей сети Интернет:

- право на свободу мысли и слова;
- право на свободу совести и вероисповедания, а так же на распространение религиозных и других убеждений;
- право на принадлежность к любой идеологии и партии;
- право на ознакомление человека с документами, затрагивающими права и свободы;
- право на поиск, хранение, распространение и другие действия с информацией в рамках, заданных федеральными законами;

– право на тайну переписки, почтовых и других сообщений;
– право на свободу прессы [3].

При рассмотрении гарантий гражданам определенных прав и свобод, провозглашенных в Конституции РФ, возникает вопрос о правовых гарантиях анонимности пользователя в Интернете. Конституция на сегодняшний момент не содержит запретительных или обязывающих норм с требованиями указывать персональные достоверные данные физического лица, позволяющие его идентифицировать, при реализации прав субъекта на свободу слова, мысли и вытекающие из них правомочия. Следовательно, пользователь при работе в сети Интернет имеет право на сохранение приватности своих личных данных, относящихся к категории персональных данных, информации и анонимности в случаях, когда соответствующие нормы явно не прописаны в законодательстве РФ (и которые присутствуют в международных правовых актах [4]). В российском законодательстве пока не существует норм, разрешающих органам власти или другим субъектам сбор сведений, в том числе и персональных данных о пользователях и их дальнейшую агрегацию в различные базы данных, как ведомственные (федеральные и муниципальные), так и частные без явного разрешения пользователя, исключение составляют специальные категории персональных данных, перечисленные в 152-ФЗ «О персональных данных» ст. 10. В международном правовом поле используются основные нормативные правовые акты ООН или других международных объединений (например, Совета Европы) [4-7].

Кроме физических лиц, к пользователям сети Интернет можно отнести различные юридические лица – предприятия и организации, которые, в свою очередь, могут являться правообладателями в отношении какой-либо информации. Несоблюдение норм и регламентов работы в Интернет, а, следовательно, нарушение анонимности сотрудниками компании может повлечь за собой как разглашение конфиденциальной информации (к примеру, коммерческой тайны), так и государственной тайны, а также многочисленные нарушения конституционных прав граждан, связанные с анонимностью.

Также пользователями Интернет могут выступать авторы – лица, занимающиеся творческой деятельностью, и юридические лица, обладающие чаще смежными правами. Для них Интернет выступает в качестве средства массовой информации, где объекты авторского права могут быть представлены для ознакомления, как на некоммерческой, так и на коммерческой основе, поэтому, рассматриваемая категория лиц заинтересована в возможности подтверждения своих прав, что противоречит анонимности. В то же время отсутствие анонимности в сети может привести к нежелательным последствиям, как для авторов, так и для потребителей результатов интеллектуального труда. Результаты интеллектуальной деятельности и средства индивидуализации в РФ регулируются нормами ч. IV Гражданского Кодекса РФ.

При анализе проблемы с точки зрения государства, можно заключить, что оно не только защищает права пользователей сети Интернет согласно Конституции, Уголовному Кодексу и другим законам, но и осуществляет противодей-

ствие источникам возможных угроз для общества в целом. К таким угрозам относят терроризм, экстремизм, пропаганду войны, пиратство, хакерство и так далее.

Важно отметить, что государство (его институты), в соответствии, со ст. 12 ФЗ № 148 *не может вмешиваться* в любые действия, совершаемые любым человеком над любой информацией.

Следует отметить, заинтересованность государства в правовом регулировании и контроле над информационными потоками в телекоммуникационных сетях. Проанализировав принятые и готовящиеся к принятию поправки и законы, можно сделать вывод о том, что Государство старается не только защищать своих граждан, но и получать доступ к любой информации о любом гражданине в любой момент времени под различными обоснованиями правомерности своих действий. Этот вывод справедлив для любого государства. В качестве примера можно привести ещё не принятые некоторые поправки к Гражданскому Кодексу Российской Федерации: «*не являются нарушением правил, установленных абзацем первым настоящего пункта, сбор, хранение, распространение и использование информации о частной жизни гражданина в государственных, общественных или иных публичных интересах, а также в случаях, когда информация о частной жизни гражданина ранее* ***стала общедоступной*** *либо была раскрыта самим гражданином или по его воле*».

Исходя из этих поправок, государство наделяет свои институты правом на вмешательство в переписку, переговоры и т. д. неугодных лиц.

Рассматривая данную проблему с позиции злоумышленника, стоит обратиться к Уголовному Кодексу РФ. Злоумышленником концепция анонимности может быть использована и широко используется в корыстных целях. Каждый пользователь, посещая ресурсы в Интернете, так или иначе, оставляет информацию о своей сетевой активности в сети. И если используются платные сервисы, то одной из приоритетных целей для мошенников являются личные данные пользователей. Жертвой мошенника может быть не только частный пользователь, который, к примеру, ввёл номер своей банковской карты, но и крупные организации. Это происходит отчасти и от того, что сегодня доказать факт мошенничества в сети Интернет и причастности к нему какого-либо конкретного человека становится всё сложнее. О наказаниях за мошенничество в компьютерной сфере говорится в ст. 159 УК РФ. В УК РФ глава 28 посвящена преступлениям в сфере компьютерной информации.

Доступ к информации, хранящейся на компьютере, может быть возможен не только напрямую (физический доступ к ресурсу), но и удаленно посредством сети Интернет. Этим и пользуются злоумышленники, так как осуществить проникновение и «замести следы» в Интернет намного легче, чем в реальной жизни, а значит и безопаснее и более привлекательно для потенциального преступника. Возможность анонимности в сети делает преступления в компьютерной сфере более изощрёнными и бесцеремонными .

Не трудно заметить, что в некоторых случаях наказание за уничтожение, блокирование, модификацию или копирование компьютерной информации, по-

влекшее крупный ущерб оказывается несоответственно мягким по сравнению с возможными убытками и наоборот. Судебная практика РФ показывает, что тяжелые меры наказания по ст.272-274 применяются крайне редко. В некоторых случаях требуемое прокурором наказание за совершенное правонарушение чрезмерно, но это компенсируется сложностью ведения оперативно-розыскных и прочих проводимых мероприятий и малым процентом доведенных до логического завершения уголовных дел.

В основном, действия злоумышленников направлены на:

- получение материальных средств;
- получение известности (славы);
- получение конфиденциальной информации с целью последующей её продажи или использования;
- получение конфиденциальной информации с целью её разглашения;
- вывод из строя информационной системы (вандализм).

Объектом атаки злоумышленника могут так же выступать государственные структуры, как федерального, так и муниципального уровней, а также как «своего» так и «чужого» государства. В этом случае целью подобных атак может быть не только получение данных ограниченного доступа, но и разглашение сведений, составляющих государственную тайну. Правовые отношения между пострадавшей стороной (пользователем) и злоумышленником регулирует УК РФ. На сегодняшний день применение норм УК РФ при расследовании компьютерных инцидентов или преступлений в сфере высоких технологий часто упирается в проблему анонимности злоумышленника, и, в этих случаях, анонимность несёт негативную роль в определении – персонификации субъекта, совершившего противоправное деяние и в доказуемости его причастности к преступлению. Кроме того, в УК РФ не отработана не только теоретическая, но и практическая части вплоть до проведения порядка процессуальных действий.

Так же, следует остановиться на проблеме размещения в сети информации, которая может быть рассмотрена как экстремистская. Проблема экстремизма тесно связана с проблемой анонимности. Чаще всего, люди, распространяющие экстремистские взгляды желают остаться анонимными. С одной стороны к экстремистским убеждениям можно отнести какой-либо вид религии или идеологии, которые, как правило, не отличаются терпимостью по отношению к лицам, не поддерживающим данные взгляды. Согласно Конституции [5] РФ и Всеобщей Декларации Прав Человека ООН [4], люди имеют права на распространение подобных взглядов, при условии соблюдения прав и свобод других субъектов. Но, с другой стороны, существует № 144-ФЗ «О противодействии экстремистской деятельности», согласно которому запрещается распространение экстремистской информации. Однако существуют множество дискуссий о том, какую информацию следует относить к экстремизму. Основной вывод из анализа публикаций – любую идеологию, не соответствующую государственной, можно отнести к экстремизму, так как она пропагандирует изменения основ государственного или политического строя. Так же, любое религи-

озное учение можно связать с экстремизмом, так как они разжигают религиозную рознь, утверждая религиозное неравенство или превосходство своих адептов над иными. Очевидно, что подобного рода уточнения экстремистских дефиниций можно в дальнейшем расширить с помощью дальнейших поправок к 144-ФЗ.

Имеет смысл напомнить о Едином реестре запрещённых сайтов, который находится в ведении Роскомнадзора в соответствии с постановлением Правительства Российской Федерации от 26 октября 2012 года № 1101. В данный реестр вносятся сайты, содержащие информацию, распространение которой в Российской федерации запрещено. Порядок блокировки ресурсов содержащих подобную информацию рассмотрен в ст. 15.3 № 149 - ФЗ «Об информации, информационных технологиях и о защите информации». Данная поправка разрешает досудебную блокировку сайтов, которая производится в случае получения уведомления от федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций или граждан.

Проанализировав все законодательные акты, упомянутые в данной работе, можно сделать вывод, что законодательство Российской Федерации на текущий момент не перекрывает всех возможных преступлений в компьютерной сфере, имеющих отношение к проблеме анонимности.

В процессе исследования понятия и сущности анонимности с различных позиций (пользователь, государство, злоумышленник), можно придти к некоторым умозаключениям.

Поскольку отношения между данными субъектами регулируются посредством законодательства РФ, существует дисбаланс между интересами среднестатистического пользователя и государства в лице его институтов. Пользователь в определенных случаях очень хочет сохранять анонимность, но одновременно желает быть защищённым от действий злоумышленника и иногда чрезмерной опеки государства. Эту функцию защиты в той или иной мере пользователю-гражданину гарантирует государство. По утверждению государства (его институтов), защита пользователей, а также ведение следственно-розыскных и судебных мероприятий станет существенно эффективнее при изменении и усовершенствовании законодательных основ, направленных на ограничение анонимности в обществе, а именно, на отмену (частичную или полную) возможной анонимности в сети Интернет, что, однако противоречит неизменяемым статьям Конституции РФ и основным международным актам [3-7].

Законодательная основа нигде, никогда не обеспечит абсолютную безопасность для пользователя в современном быстро меняющемся технологическом мире, следовательно, сам пользователь должен осознавать риск использования компьютерных технологий и уметь защищать свою анонимность и свои компьютерные ресурсы самостоятельно.

Литература

1 Белл, Д. Грядущее постиндустриальное общество [Текст] / Д.Белл. - М.: *Basic Books*, 2001. – 578 с.

2 Петров В. П., Петров С. В. Информационная безопасность человека и общества: учебное пособие. – М. : ЭНАС, 2007. – 336 с.

3 Конституция Российской Федерации. Принята всенародным голосованием 12 декабря 1993 года. С изм. 6-ФКЗ, 7-ФКЗ от [Текст] // Российская газета, 21.01.2009,. – Федеральный выпуск №7

4 Всеобщая декларация прав человека [Электронный ресурс] - Режим доступа: *http://constitution.garant.ru/act/right/megdunar/2540400/,* свободный - Яз., рус. – Загл с экрана.

5 Международный пакт о гражданских и политических правах [Электронный ресурс] - Режим доступа: *http://constitution.garant.ru/act/right/megdunar/2540400/*, свободный - Яз., рус. – Загл с экрана.

6 Конвенция о защите прав человека и основных свобод ETS N 005 [Электронный ресурс] - Режим доступа: *http://constitution.garant.ru/act/right/megdunar/2540400/*, свободный - Яз., рус. – Загл с экрана.

7 Хартия социальных прав и гарантий граждан независимых государств. [Электронный ресурс] - Режим доступа: *http://constitution.garant.ru/act/right/megdunar/2540400/*, свободный - Яз., рус. – Загл с экрана.

Д.В. Литвинов

ИССЛЕДОВАНИЕ ОПТИМАЛЬНОЙ СТРАТЕГИИ КЛАССИФИКАЦИИ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ НА ОСНОВЕ ГРАФА ПОТОКА ВЫПОЛНЕНИЯ

(Центр специальных разработок Министерства Обороны РФ)

Введение

Вредоносное ПО представляет серьезную угрозу для современных компьютерных систем. Все вредоносные программы можно разделить на семейства со схожей функциональностью. Целью классификации вирусов является как поиск новых семейств, так и определение принадлежности образца к уже существующему семейству.

В данной работе сравнивается эффективность двух стратегий классификации с целью поиска наиболее оптимального в смысле некоторого критерия. Под стратегией классификации в дальнейшем будем понимать способ определения расстояния между графами (с помощью марковских цепей и расстояния редактирования) и алгоритм кластеризации набора вредоносных программ на семейства (метод k средних и DBSCAN).