КОНТЕКСТ КАК ИНДИКАТОР ВРЕДОНОСНОГО КОНТЕНТА

В.Н. Максименко, *к.т.н., доцент, Московский технический университет связи и информатики, vladmaks@yandex.ru.*

УДК 004

Аннотация. Качество информационных услуг оценивается на этапах обработки и передачи. Для расчета стандартных показателей качества «из конца в конец» учитывают только показатели технических средств. Считается, что информация всегда является правдивой. С развитием социальных сетей и электронных средств доставки возросли требования к защите конфиденциальной информации. Существующие методы защиты конфиденциальной информации, использующие шаблоны документов или ключевые слова, не учитывают контекст, который помогает оценить полезность информации по таким критериям как хороший – плохой, правдивый – ложный, интересный – скучный.

Ключевые слова: контент; контекст; доверие; защищенность информации; качество информационной услуги.

CONTEXT AS AN INDICATOR OF MALICIOUS CONTENT

Vladimir Maximenko, *Ph.D., Associate Professor, Moscow technical university of communications and informatics.*

Annotation. The quality of information services is assessed at the stages of processing and transmission. To calculate the standard quality indicators "from end to end", only the indicators of technical means are taken into account. It is believed that the information is always true. With the development of social networks and electronic means of delivery, the requirements for the protection of confidential information have increased. Existing methods of protecting confidential information using document templates or keywords do not take into account the context, which helps to assess the usefulness of information by criteria such as good – bad, truthful – false, interesting – boring.

Keywords: content; context; trust; information security; quality of information services.

Введение

Сочетание компьютерных, телекоммуникационных, информационных и навигационных технологий создает предпосылки для создания высокопроизводительных распределенных информационных систем и систем реального масштаба времени. Класс инфокоммуникационных услуг сетей сотовой подвижной связи (СПС) характеризуется тем, что предоставляется путем последовательного использования технологических свойств специальных серверов приложений и сетевых сервисов СПС. Использование технологий искусственного интеллекта становится одним из приоритетных направлений в защите информации и инфраструктуры распределенных информационных систем и сетевых приложений. Специфика информационной безопасности состоит в том, что она является составной частью информационных технологий – области, развивающейся очень высокими темпами, при этом современные технологии программирования не позволяют создавать безошибочные программы, что приводит к появлению уязвимостей информационной системы. В

инфокоммуникационной услуге к сетевой составляющей услуги относится только доступ абонента в сеть оператора, остальная же часть услуги предоставляется с помощью серверов сети. Обобщенная структурная схема сети связи с оказанием информационных услуг приведена на рис. 1.

Информационная безопасность в показателях качества услуг

Качество абонентской услуги зависит от качества на каждом шаге оказания услуги [1]. Например, доступность абонентской услуги определяется не только доступностью сети, но и доступностью каждого из серверов, участвующих в процессе оказания услуги.

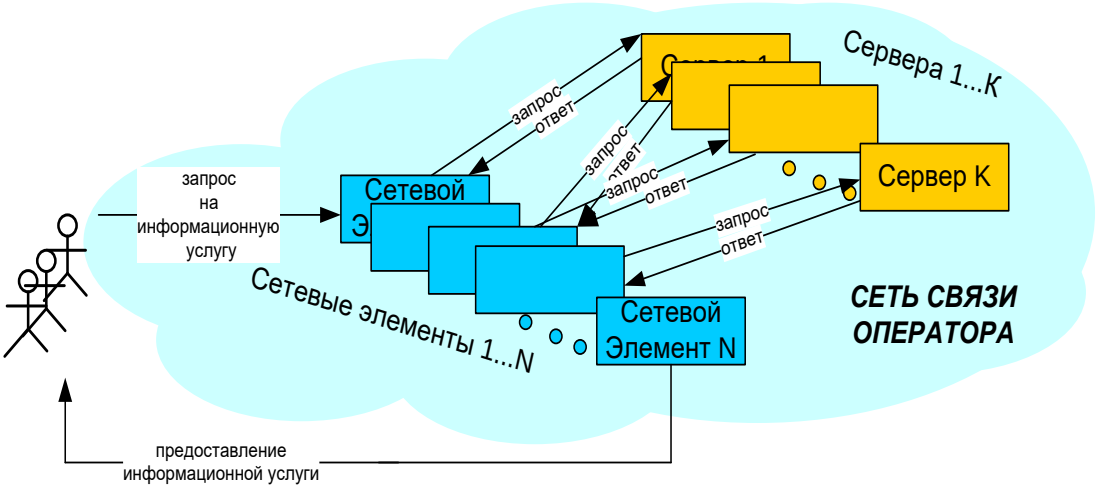

Рисунок 1

Для того чтобы оценить качество такой абонентской услуги в стандартизованных категориях (доступность, целостность, непрерывность), используют метод ее декомпозиции на элементы, качество которых поддается оценке в указанных категориях качества. Для таких элементов вводится понятие «сервис». Ограничиваясь пока только техническими аспектами качества абонентской услуги, под сервисами понимаются отдельные технологические свойства сетевых элементов, с использованием и во взаимодействии которых предоставляется абонентская услуга. Сами сетевые элементы выступают в качестве ресурсов. На рис. 1 представлена обобщенная структурная схема сети связи с оказанием информационных услуг.

Проектирование информационных услуг на сетях подвижной связи начинается с разработки диаграммы вариантов использования. Главный прецедент определяет основную цель информационной услуги. Вспомогательные прецеденты определяют требования, которые должны быть выполнены для достижения цели.

Обобщенная диаграмма прецедента услуги на основе определения местоположения приведена на рис. 2. Требования информационной безопасности на диаграмме рис. 2 представлены прецедентами авторизации и получение доступа к системе, реализующей информационную услугу.

Первое, с чем сталкивается пользователь при доступе к любому информационному сервису является проверка превентивными мерами информационной безопасности сервиса аутентификации. Существует множество механизмов аутентификации, каждый из которых можно оценить посредством качественных показателей доступности, таких как вычислительная сложность и время проверки. Сервисы безопасности используются и на других этапах

обработки и передачи информации при оказании услуг, и поэтому должны учитываться при оценке качества информационных услуг.

Для того чтобы управлять информационной безопасностью необходимо выполнить ряд операций сбора, обработки и выдачи управляющих воздействий в информационной системе.

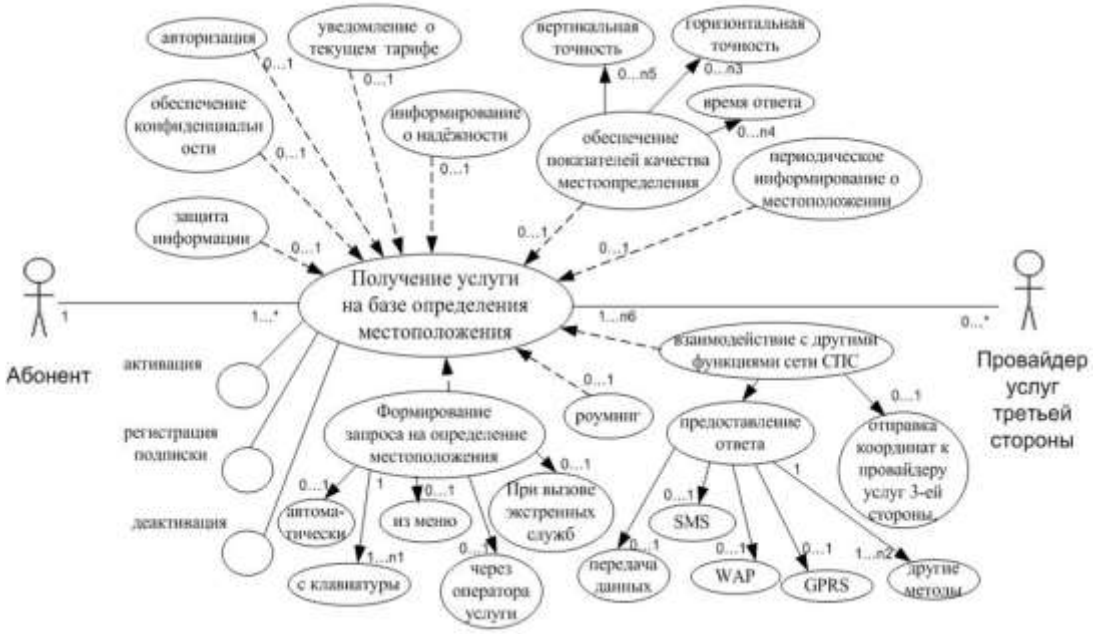

Рисунок 2

Основную часть этих действий выполняет система мониторинга. Система мониторинга – это система, которая работает с большим количеством информации в реальном масштабе времени. Для снижения требований производительности системы мониторинга используют принцип декомпозиции по функциональному принципу, используя показатели: ресурсы, сервисы и услуги (приложения) [2].

Концептуальная модель подсистемы информационной безопасности представляет собой *UML*-диаграмму классов. Основными действующими лицами являются: владелец системы и злоумышленник (агент угроз). Учитывая функциональною декомпозицию, активы компании представлены в виде классов ресурсов сети, сервисов сети и услуг связи, образующими классы инвентаризации ресурсов, сервисов и услуг.

Агент угрозы создает угрозы, которые направлены на ресурс сети, сервис сети или/и услуги сети используя, для этого имеющиеся в информационной системе уязвимости. Каждая угроза безопасности увеличивает информационные риски, которые могут привести к потерям ресурсов, сервисов и услуг системы. Очевидно, что наибольший ущерб наносят угрозы, направленные на ресурсы сети.

Роль контекста в показателях качества контента (услуг)

Контент может состоять из разной информации: хорошей и плохой, правдивой и ложной, интересной и скучной. Но необходимо, чтобы этот контент был полезен тем людям, которым он адресован. Под нежелательным можно считать контент, содержащий информацию, которая может навредить человеку психологически, а также содержащий призывы к действиям, которые могут нанести вред самому человеку или же иному лицу (группе лиц).

Контент сайта – это любая информация, размещенная на нем. Без качественного и регулярного обновляемого контента практически невозможно повысить эффективность онлайн-бизнеса и вывести сайт в топ поисковых рейтингов. Любая информация, которую сайт предлагает пользователю должна быть полезной. Контент сайта – это его информационное наполнение. Содержимое сайта должно соответствовать уровню целевой аудитории.

Содержимое сайта должно периодически меняться, чтобы привлекать внимание. Если нет положительной информации, то используют отрицательную зловредную информацию. Поэтому необходимо разработать методы обнаружения зловредного злонамеренного контента. Качество услуги или информационной безопасности оценивается показателями доступности, целостности и конфиденциальности. Эти показатели не отражают свойства самой информации, насколько она является истинной или ложной. Оценить это можно только по косвенным признакам, таким как компетентность автора в области рассматриваемой информации, и комментарии читателей, на сколько мы можем доверять автору и читателям – субъектам информационных отношений. Этот вопрос выходит за пределы оценки качества и информационной безопасности информационной системы и находится в области оценки доверия к субъектам информационных отношений.

Полезность информации определяется ее истинностью или ложностью для отдельного субъекта информационных отношений или отдельной организации. Информация делится на общедоступную и конфиденциальную. Конфиденциальная информация является объектом защиты. Одним из методов нарушения конфиденциальной информации является передача такой информации с нарушением политики безопасности. Признаки конфиденциальной информации – шаблоны документов или ключевые слова, которые образуют библиотеку критериев информационной безопасности. Автоматизация выявления защищаемой информации обеспечивается путем сравнения контента с перечнем шаблонов и ключевых слов.

Основные методы выявления нежелательного контента для таких информационных материалов, как текст и изображение сводятся к очистке текста от служебных символов языка разметки гипертекста *HTML* и передаче очищенного текста для последующего сравнения слов текста с ключевыми словами из списка нежелательных слов.

Совпадение слова на странице со словом из некоторого списка нежелательных слов увеличивает негативный рейтинг текста. Когда относительное количество нежелательных слов превышает заданный порог, то делается вывод о том, что контент на данном веб-сайте относится к нежелательному [3]. Другие методы основаны на похожести одного текста на другой. Здесь не проверяется наличие в тексте чего-то заранее определенного негативного, а выполняется сравнение текстов. Похожесть может оцениваться по-разному, чаще всего речь идет о принадлежности текста к какой-то категории, т.е., сводится к задаче классификации [3, 4].

В последнее время шаблон документа и состав ключевых слов в нем не в полной мере обеспечивают защищенность конфиденциальной информации. Очень многое зависит от контекста, т.е. от обрамления контента, от того, кто является источником информации и в каких условиях и среде эта информация появилась. На первый план выходит показатель доверия. В докладе представлен анализ типов доверия и обзор алгоритмов методов оценки доверия.

Социальная сеть – это программно-техническая платформа для функционирования социальных сообществ, в которых зарегистрированные

пользователи социальной сети объединяются в устойчиво функционирующие группы на основе взаимных интересов отдельных членов сообщества или степени доверия к источникам информации.

В настоящее время можно выделить три основных типа доверия: субъект-объект, объект-объект и субъект-субъект. В качестве «субъекта» выступает «человек», а «объектом» является «компьютер». Доверие среди пользователей в социальных сетях представляет большой интерес в области информационной безопасности. Поскольку социальные сети зачастую используют для распространения мнений определенной направленности, что объясняется пониженной критичностью восприятия пользователями информации [3]. Знания о доверии в социальных сетях также могут использоваться в системах рекомендаций.

Есть два основных типа доверия: прямое доверие и доверие к рекомендациям. Прямое доверие – доверие на основании личного опыта. Доверие к рекомендациям – доверие, основанное на мнении авторитета, группы людей, пропаганды (если *A* доверяет *B*, а *B* доверяет *C*, то *A* в некоторой степени тоже доверяет *C*) [5].

Существует три важных аспекта доверия: доверие зависит от поведения пользователя, доверие является динамичным и доверие зависит от контекста.

Важный элемент определения социального доверия – это контекст. Например, член *X* в сообществе доверяет рекомендациям другого члена *Y* по поводу автомобилей. Но в то же время, *X* не может доверять рекомендациям *Y* по поводу компьютерных игр или музыки.

Другим важным аспектом доверия является то, что оно зависит от времени. Взаимодействие, которое произошло в последнее время, может иметь большую ценность чем те, которые произошли некоторое время назад. Поэтому время является важным фактором для фиксации изменения в поведении индивида. Например, член *X* может иметь хорошие отношения с другим членом *Y* во время *t*, но эта связь может ослабевать, при отсутствии взаимодействия между ними.

Существует два типа взаимодействий: активный и пассивный. Пример активного взаимодействия включает в себя большое количество друзей, регулярные публикации, комментирование других членов и т.д. Однако не все члены сообщества – активные участники. Есть значительное количество членов, которые являются пассивными участниками сообщества. Взаимодействие пассивных членов в сообществе включает чтение статей, регулярные посещения сообщества и т.д. Эти члены могут не участвовать или не делиться своим опытом или чувствами, но они являются потребителями информации, что тоже очень ценно. Эти два типа взаимодействия коллективно создают социальный капитал сообщества и используются для оценки социального доверия.

Заключение

Без доверия люди не захотят делиться своими знаниями и опытом из-за страха, что их публикации и идентификационные данные будут использованы неправильно или даже незаконно. Таким образом, актуальной становится задача построения сети доверия. Алгоритмы путей создания сообществ доверия в социальной сети представлены в работе [5]. Реализация этих путей представляет сложную задачу по сбору исходных данных и автоматизации обработки.

Литература

1. Максименко В.Н., Васильев М.А. Методика расчета стандартных показателей качества дополнительных услуг на сетях подвижной связи // T-Comm: Телекоммуникации и транспорт, 2011. – Т. 5. – № 4. – С. 26-28.
2. Максименко В.Н. Конвергенция сервисов качества и защиты информации в сетях сотовой подвижной связи на этапах проектирования // T-Comm: Телекоммуникации и транспорт, 2018. – Т. 12. – № 11. – С. 57-64.
3. Шелухин О.И., Смычек М.А., Симонян А.Г. Фильтрация нежелательных приложений интернет-ресурсов в целях информационной безопасности // «Наукоемкие технологии в космических исследованиях, 2018. – Т. 10. – № 2. – С. 87-98.
4. Галимова А.Г., Симонян А.Г. Методы выявления нежелательного контента в тексте и изображениях // Сборник трудов XV Международной отраслевой научно-технической конференции «Технологии информационного общества». Москва. 03-04 марта 2021. – С. 151-152.
5. Максименко В.Н., Долгова Н.Д. Анализ алгоритмов вычисления уровня доверия к пользователю в социальной сети // Экономика и качество систем связи, 2018. – № 4 (10). – С. 23-30.