

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

Николаева К.И. Защита персональных данных в сети Интернет // Материалы по итогам Всероссийской научно-практической конференции «Актуальные вопросы развития современного образования: теория и практика», 01-10 апреля 2016 г. – 0,4 п. л. – URL: http://akademnova.ru/publications_on_the_results_of_the_conferences

СЕКЦИЯ: ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ XXI века

Николаева К.И

студентка 2-го курса

специальности «Программирование

в компьютерных системах»

ГАПОУ «Бугурусланский нефтяной колледж »

Научный руководитель: Капаева О.М.

преподаватель информационных технологий

г. Бугуруслан, Оренбургская область

Российская Федерация

Защита персональных данных в сети Интернет

Интернет стал одним из главных источников информации, опередив телевидение и радио. Для многих интернет-общение эффективно заменяет телефон и почту. Возможности Интернета безграничны: поиск необходимой информации, купля-продажа, общественные связи, онлайн-общение, обучение и т.д.

Актуальность исследования

Сегодня вопрос, касающийся защиты персональных данных субъектов в сети Интернет, является актуальным. В первую очередь это связано с

невысоким уровнем грамотности населения в вопросах безопасности собственных персональных данных. Пользователи уже давно перестали следить за безопасностью своих персональных данных в интернете, но когда речь заходит об утечки данных, то возникает паника что делать или как этого избежать.

Цель исследования

Целью исследования является изучение способов защиты персональных данных в сети Интернет

Задачи исследования:

- определить, что понимается под персональными данными;
- изучить, как передаются наши данные;
- узнать существуют ли документы или законы о защите персональных данных;
- провести опрос среди студентов колледжа
- формирование на этой основе теоретических выводов и практических предложений по совершенствованию защиты персональных данных

Методы исследования

При написании данной исследовательской работы применён теоретический метод и анкетирование.

Значение исследования

Теоретическая значимость данной работы заключается в изучении системы защиты персональных данных в сети Интернет. Практическая значимость написания данной работы заключается в возможности применения теоретических и практических предложений по защите персональных данных всем пользователям сети Интернет.

Что такое персональные данные?

Персональные данные – любая информация, которая относится к определенному или определяемому физическому лицу, в том числе:

1. фамилия, имя, отчество,
2. год, месяц, дата и место рождения,
3. адрес, семейное, социальное, имущественное положение, образование, профессия, доходы.

То есть Согласно базовому закону персональными данными является абсолютно любая информация. При этом пароли к аккаунтам не являются персональными данными, так как не сообщают ничего о человеке. С согласия пользователя данные могут становиться общедоступными – например, номер телефона или e-mail, которые вы передаёте компании. При этом по требованию пользователя эти данные должны быть убраны из общего доступа. Лица, виновные в нарушении требований Федерального закона, несут гражданскую, уголовную, административную, дисциплинарную предусмотренную законодательством Российской Федерации ответственность.

Где хранятся данные?

Большинство серверов крупнейших интернет компаний находятся в Америке. В связи с новым законом, по которому российское правительство обязует компании хранить данные российских пользователей только на территории страны. Однако пока зарубежные интернет компании не комментируют их будущую работу в России, и в СМИ время от времени появляется информация о том, что власти ведут переговоры с Facebook, Google, Twitter и другими интернет компаниями.

Как передаются персональные данные?

За свободный интернет и бесплатные сервисы пользователи платят данными. Крупные компании такие как Google и «Яндекс» синхронизируют информацию из различных источников, чтобы точнее определить предпочтения пользователя. Они зарабатывают на рекламе, и чем понятнее будут интересы пользователя, тем более точное объявление можно ему показывать.

Ваши персональные данные с Вами повсюду в сети

Для выхода в сеть на компьютере имеется сетевая карта, в которую вшит MAC адрес. При подключении к интернету компьютеру присваивается IP адрес. Эти данные путешествуют с Вами по сети и по ним Ваш ПК однозначно идентифицируется, т.е. они по сути являются Вашими сетевыми паспортными данными. К этим данным легко привязать Ваше ФИО. Вы это делаете добровольно, заполняя контракт со своим интернет – провайдером или регистрируясь под своим именем на любом сайте. Хотя такая привязка не обязательна. Но к этим Вашим идентификационным данным прикрепляется вся информация, которую Вы отсылаете через сеть.

Для многих интернет – неиссякаемый источник разного рода информации. Но уже на этапе поиска нужной информации начинается слежка за Вами. Например, после того как в поисковой выдаче Google Вы нажимаете на интересующую Вас ссылку, вместе с Вашим поисковым запросом на выбранный сайт отсылаются и Ваши персональные данные. На этом сайте может фиксироваться, кто приходил и чем интересовался. Кроме того, при переходе по рекламным баннерам на сайты рекламодателей Вы также оставляете там персональные данные и информацию о Ваших интересах. По разбросанной таким образом в сети информации создаются профили о Вас.

После чего одна и та же назойливая реклама будет преследовать вас везде, куда бы Вы ни пошли.

Слежка в сети

Слежка в сети может осуществляться с помощью аппаратных и программных средств:

– аппаратный уровень. Функционирование интернета невозможно без физической реализации сети с помощью технического оборудования

– программный уровень. Для серфинга по сети или общения мы используем различные программы, такие как браузеры, Skype и т.п.

Для отслеживания информации часто используются Куки.

Куки – это файлы текстового формата. Поначалу они выполняли только полезные функции и предназначались для сохранения рабочей информации о пользователях интернет – ресурса. Например, посещал ли пользователь ранее данный ресурс. Но, чтобы не перегружать этой информацией сервера компании, Куки сохраняются на жестком диске ПК самого пользователя. Позже Куки стали использоваться для фиксации всей информации, т.е. для шпионажа. Всю информацию, которую о нас собирают, мы добровольно храним у себя на своем же компьютере.

Как государство защищает данные россиян?

Персональные данные относятся к информации ограниченного доступа и должны быть защищены в соответствии с законодательством РФ. Организации и отдельные люди, которые хранят, собирают, передают или обрабатывают персональные данные, по закону относятся к операторам персональных данных

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

На сегодня вопрос, касающийся защиты персональных данных субъектов в сети Интернет, является актуальным. В первую очередь это связано с невысоким уровнем грамотности населения в вопросах безопасности собственных персональных данных. Но начиная с 1 сентября 2016 года интернет – сервисы, которые имеют дело с персональными данными россиян, должны обеспечить возможность обработки таких сведений с использованием баз данных, находящихся в России. Данное правило вводится Федеральным законом от 21 июля 2014 г. № 242 – ФЗ. Документ коснется, прежде всего, интернет – магазинов, социальных сетей, и другие сервисов. Причем речь идет как о российских компаниях, которые хранят данные за рубежом, так и об иностранных организациях, которые имеют дело с клиентами из России. Как и следовало ожидать, Закон вызвал довольно бурную реакцию в сетевом сообществе и в среде экспертов интернет – индустрии. Традиционно авторов документа обвиняют в том, что он практически нереализуем, и на практике ни в коей мере не обеспечит безопасность россиян, а скорее усложнит им жизнь и затормозит развитие Рунета.

Причина принятия Закона формулируется в том, что многие граждане зарегистрированы в социальных сетях, покупают товары и получают услуги через Интернет. Значительная часть таких сервисов находится за границей, преимущественно в США и Европе.

Главная задача Закона – обеспечить безопасность персональных данных россиян.

По данной теме, среди студентов нашего колледжа был проведен опрос.

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

1) Знаете ли вы, что существует специальное государственное ведомство, которое должно защищать россиян от незаконного распространения и использования их персональных данных?

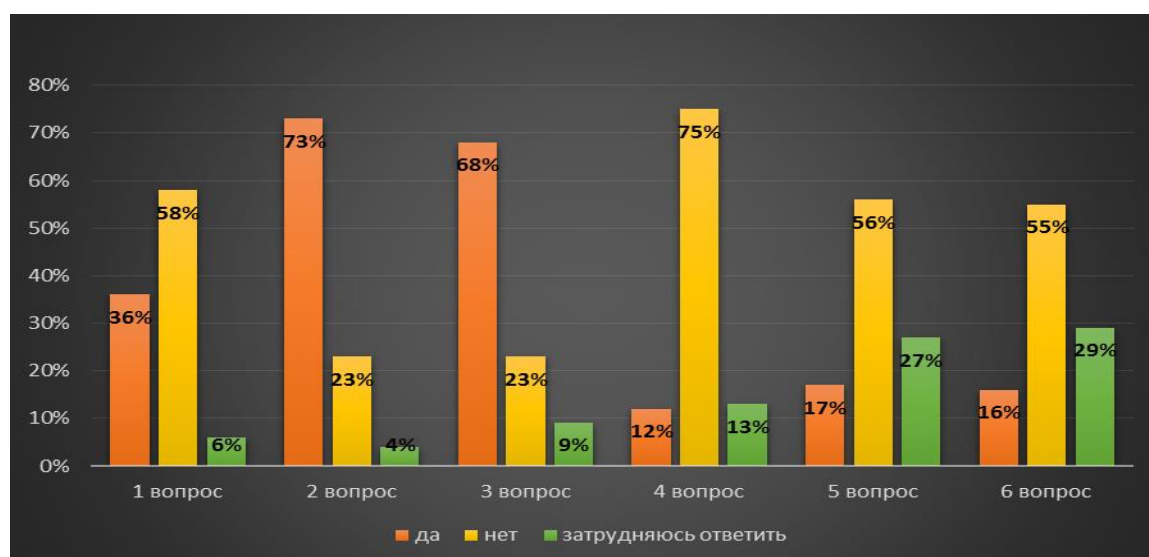
2) При заполнении бумажных документов вы обычно обращаете или не обращаете внимание на информацию о том, как будут использоваться ваши персональные данные?

3) Если вы пользуетесь интернетом, то указывая свои персональные данные на интернет – сайтах (номер телефона, кредитной карты, паспорта и т.д.), вы обращаете или не обращаете внимание на информацию о том, как они будут использоваться?

4) Как вы считаете, хорошо ли персональные данные защищаются от незаконного использования в России?

5) Приходилось ли вам сталкиваться с нарушениями персональных данных, или сталкивались с этим ваши знакомые?

6) Знаете ли вы, какое ведомство отвечает за защиту персональных данных?



По итогам опроса можно сделать выводы, что большинство студентов нашего колледжа не знают, что существуют документы и законы о защите персональных данных. Так же они абсолютно уверены, что данные совершенно не защищены от незаконного их использования.

Как пользователю сохранить свои данные от утечек и слежки?

Пользователи уже давно перестали следить за безопасностью своих персональных данных в интернете, но когда речь заходит о таких темах, как об анонимности в интернете то сталкиваешься с откровенным равнодушием. Большинство недоуменно заявляет: «А мне скрывать нечего».

Но когда речь заходит о таких темах, как защита персональных данных в интернете, об анонимности в интернете и т.п., где подчеркивается необходимость максимального сокрытия информации, связанной непосредственно с собой любимым, то сталкиваешься с откровенным равнодушием. Большинство недоуменно заявляет: «А мне скрывать нечего».

Через сеть собирают информацию государственные разведки и спецслужбы, занимаются конкурентной разведкой коммерческие, банковские структуры, собирают сведения и формируют пользовательские профили рекламные и торговые фирмы, шпионят частные лица. Несанкционированным сбором информации занимаются самые известные поисковые системы, социальные сети и большинство сайтов, которые Вы посещаете.

О масштабах проблемы можно судить по обширному количеству средств противодействия. Все самые популярные браузеры имеют режим инкогнито, препятствующий слежению за пользователем в сети. При том, что среди браузеров идет жесткая конкуренция по показателям быстродействия.

Возникает резонный вопрос: «Где же хранить такие огромные объемы информации о каждом пользователе сети?» Самое веселое в ответе на этот вопрос является то, что огромную долю этой информации мы храним сами на собственных компьютерах.

Заключение

Подводя итоги вот несколько советов, которые помогут защитить важные данные:

1. старайтесь не посещать сомнительных сайтов в интернете;
2. используйте антивирусы;
3. пользуйтесь настройками приватности, давайте ограниченный доступ к вашим данным и предоставляйте его только тем людям, с которыми вы знакомы лично и в которых можете быть на сто процентов уверены;
4. не ленитесь читать все условия соглашений и варианты опций, потому что там всегда можно найти что-нибудь, что позволит сторонним людям на законных основаниях собирать о вас все персональные данные.
5. полностью заблокируйте всплывающие окна, настройте оповещения при попытке зайти на небезопасный сайт;
6. заблокируйте передачу данных и куки третьим сторонам и различным рекламным сервисам, а самое главное – везде при возможности выбирать опцию «Не отслеживать» - это заблокирует для сайтов возможность сбора вашей персональной информации;
7. внимательнее обращайтесь с «бесплатными» приложениями и программами, так как в итоге вы рискуете поплатиться за неосторожность, начинается все с обилия рекламы, расположенной прямо в приложении, и заканчивается тем, что многие из них получают возможность собирать ваши данные, как только вы устанавливаете их на свой компьютер или смартфон;

Всероссийское СМИ

«Академия педагогических идей «НОВАЦИЯ»

Свидетельство о регистрации ЭЛ №ФС 77-62011 от 05.06.2015 г.

(выдано Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций)

Сайт: akademnova.ru

e-mail: akademnova@mail.ru

8. сложный пароль, который легко запомнить. Сложность пароля определяется, прежде всего, его длиной – чем длиннее пароль, тем сложнее его подобрать;

9. защитите информацию от случайных посторонних;

10. регулярно осуществляйте обновление программ, обеспечивающих безопасность вашей операционной системы, лучше всего выбрать вариант автоматического получения важных обновлений.

Если вы будете придерживаться этих советов, ваши персональные данные будут в безопасности.

Список использованной литературы

1) Мельников В.П., Клейменов С.А., Петраков А.М. Информационная безопасность и защита информации. 3-е изд., стер. - М.: 2008. — 336 с.

2) Таненбаум Э. Современные операционные системы. 3-е изд. - СПб.: 2010. — 1120 с.

3) Петренко С.А., Курбатов В.А. - Политики безопасности компании при работе в интернет. ДМК Пресс. 2011.

4) <http://rg.ru/2006/07/29/personaljnye-dannye-dok.html>

5) <http://base.garant.ru/997729/>

Опубликовано: 01.04.2016 г.

© Академия педагогических идей «Новация», 2016

© Николаева К.И., 2016