

УДК 34.00.00

**Липовская Юлия Владимировна**

студентка 1 курса группы 18-СПО-ПД-02

Академия маркетинга и социально-информационных технологий –ИМСИТ  
(Краснодар)

научный руководитель к.г.н, доцент: А.Н. Сотниковой.

### **«ПРАВОВЫЕ АСПЕКТЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНТЕРНЕТЕ»**

**Аннотация.** В работе рассмотрены актуальные проблемы связанные с защитой конфиденциальной информации во Всемирной сети Интернет, а так же риски утечек и методы защиты.

**Ключевые слова.** Актуальные проблемы защиты информации в Интернете, методы защиты конфиденциальной информации.

**Abstract:** In work current problems the risks of leaks and methods of protection connected with protection of confidential information in Worldwide network Internet, and also are considered.

**Keywords:** Current problems of information security on the Internet, methods of protection of confidential information.

21 век-время компьютерных технологий. С каждым годом общество всё больше предпочитает переходить на новейшие гаджеты и познавать огромные масштабы Всемирной паутины. На сегодняшний день количество пользователей Интернета достигает свыше 3,5 миллиарда человек, а это половина населения всего Земного шара. Жизнь современного человека “летит” не по дням, а по часам, и гаджеты помогают экономить время и значительно упрощают нашу жизнь. Мы оплачиваем покупки, привязывая банковские счета к телефону, общаемся через мессенджеры, храним фотографии в “облаке” и многое другое. Каждый из нас хочет, чтобы вся наша личная информация имела право на конфиденциальность. Но, к сожалению, на данный момент интернет является самым не безопасным хранилищем данных.

Конфиденциальная информация, которая передается по сети Интернет, проходит через определенное количество маршрутизаторов и серверов, прежде чем достигнет пункта назначения. Обычно маршрутизаторы не отслеживают проходящие сквозь них потоки информации, но возможность того, что

информация может быть перехвачена, весьма велика. Более того, информация может быть изменена и передана адресату в измененном виде. Крупные утечки информации происходят каждый год (начиная от взлома страниц в соц.сетях и до взлома десятка тысяч банковских счетов и информации банка). Интернет-маньяки могут получить нужную им информацию за пару часов. Так как, например, в 2016 году хакер под псевдонимом Le4ku заявил, что взломал сайт Федерального бюро расследований (ФБР) США. И это далеко не единичный случай.

Способы защиты информации включают использование аппаратных средств и устройств, а также внедрение специализированных технических средств и программного обеспечения. Электронная почта - самая распространенная услуга сети Internet. В настоящее время свой адрес по электронной почте имеют приблизительно 20 миллионов человек. Посылка письма по электронной почте обходится значительно дешевле посылки обычного письма. Более того, сообщение, посланное по электронной почте, дойдет до адресата за несколько часов, в то время как обычное письмо может добираться до адресата несколько дней, а то и недель.

Защита информации — это деятельность по предотвращению утечки, хищения, утраты, модификации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. По техническим и неумышленным причинам, под это определение подпадает также деятельность, связанная с повышением надежности сервера из-за отказов или сбоев в работе винчестеров, недостатков в используемом программном обеспечении и другое.

Безопасность данных является одной из главных проблем в Интернете. Появляются все новые и новые страшные истории о том, как компьютерные взломщики, использующие все более изощренные приемы, проникают в чужие базы данных. Разумеется, все это не способствует популярности Интернета в деловых кругах. Одна только мысль о том, что какие-нибудь хулиганы или, что еще хуже, конкуренты, смогут получить доступ к архивам коммерческих данных, заставляет руководство корпораций отказываться от использования открытых информационных систем. Специалисты утверждают, что подобные опасения безосновательны, так как у компаний, имеющих доступ и к открытым, и частным сетям, практически равные шансы стать жертвами компьютерного террора. Каждая организация, имеющая дело с какими бы то ни было ценностями, рано или поздно сталкивается с посягательством на них. Предусмотрительные начинают планировать защиту заранее,

непредусмотрительные - после первого крупного “прокола”. Так или иначе, встает вопрос о том, что, как и от кого защищать.

Методы и способы защиты информации содержат в себе конкретные меры и технологии к решению проблем по информационной безопасности предприятия. На текущий момент методы защиты можно разделить на несколько основных групп. На практике используют несколько групп методов защиты:

- 1)препятствие на пути предполагаемого похитителя; препятствие создают физическими и программными средствами;
- 2)управление, или оказание воздействия на элементы защищаемой системы;
- 3)маскировка, или преобразование данных, обычно – криптографическими способами;
- 4) разработка нормативно-правовых актов и набора мер, направленных на то, чтобы побудить пользователей, взаимодействующих с базами данных, к должному поведению;
- 5) создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;
- б) создание условий, которые мотивируют пользователей к должному поведению.

Каждый из методов защиты информации реализуется при помощи различных категорий средств. Основные средства – организационные, программные, и технические.

В ходе развития концепции защиты информации специалисты пришли к выводу, что использование какого-либо одного из выше указанных способов защиты, не обеспечивает надежного сохранения информации. Необходим комплексный подход к использованию и развитию всех средств и способов защиты информации.

Интернет стал неотъемлемой частью нашей жизни, и в данной работе была рассмотрена мною проблематика защиты информации в данной глобальной сети. Эта проблема была и останется актуальной еще не один год, так как никто еще не может нам гарантировать на 100% того, что наша информация будет надежно защищена или в наш компьютер не попадёт вирус. Наблюдаемый в

последние годы взрывной рост популярности Интернета и связанных с ним коммерческих проектов послужил толчком для развития нового поколения технологий защиты информации в IP-сетях. Причем если ранее, вплоть до начала 90-х, основной задачей защиты в Интернете было сохранение ресурсов преимущественно от хакерских атак, то в настоящее время актуальной становится задача защиты коммерческой информации. Сохранение конфиденциальности информации очень важно, и чтобы не допускать утечек, мы должны соблюдать определённые требования, которые мы разобрали в этом проекте.

### Литература

1. Герасименко В. А. Защита информации в автоматизированных системах обработки данных: развитие, итоги, перспективы. Зарубежная радиоэлектроника, 2003, № 3.
2. Закер К. Компьютерные сети. Модернизация и поиск неисправностей. СПб.: БХВ-Петербург, 2001.
3. Галицкий А. В., Рябко С. Д., Шаньгин В. Ф. Защита информации в сети - анализ технологий и синтез решений. М.: ДМК Пресс, 2004. - 616 с.
4. Браун С. “Мозаика” и “Всемирная паутина” для доступа к Internet: Пер. с англ. - М.: Мир: Малип: СК Пресс, 1996. - 167с.
5. УК РФ Глава 28. ПРЕСТУПЛЕНИЯ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ