АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Созыкин Александр Семенович

студент, Тюменский государственный университет, РФ, г. Тюмень

Сахно Александр Иванович

научный руководитель, канд. юрид. наук, Тюменский государственный университет, РФ, г. Тюмень

Информация в наше время является самым ценным ресурсом, а в современном мире в эпоху развития компьютерных технологий защита информации как никогда актуальна, так как ежедневно появляются новые способы завладения конфиденциальной информацией, а также развиваются вредоносные программы, с помощью которых злоумышленники легко завладевают чужими данными, представляющими для них ценность.

Незаконных хакерских методов завладения чужой информацией огромное множество: это и вирусные программы, проникающие в программные обеспечения устройств пользователей, которые об этом даже не подозревают; и рассылка не запрошенной корреспонденции, иначе говоря, спам-писем, поступающих в почтовые ящики адресатов, а также пользователям мессенджеров; и звонки из банков, которых даже не существует.

К сожалению, в том, что сейчас происходит, во многом виноваты и сами люди – пользователи благ Интернет - пространства, собственноручно загружающие всю информацию о своих персональных данных в Интернет, которую потом не составляет труда найти с помощью тех же самых поисковиков. Так, в Интернете хранится большое количество личной информации: фотографии, банковские реквизиты, адреса мест работы или адреса мест жительства, номера телефонов, трудовые книжки, медицинские карты и даже паспортные данные. Заполучив хотя бы часть из вышеперечисленных данных, злоумышленник может по цепочке узнать все о владельце такой информации и в итоге обратить ее против него же.

Однако не всегда личная информация попадает в Интернет с согласия ее владельцев, к примеру, на практике бывают случаи, когда компании «продают» данные своих клиентов или же бывают случаи, когда хакеры удаленно подключаются к чужим персональным компьютерам и заполучают всю информацию, хранившуюся на устройствах.

Почему же так происходит? Почему никто не может остановить злоумышленников и обеспечить информационную безопасность в полной мере?

Вообще обеспечение информационной безопасности это не только внутригосударственная проблема, это проблема мирового масштаба и доказательством тому может быть принцип, содержащийся в статье 17 международного пакта о гражданских правах и политических правах[1]. Так, пактом установлено, что «никто не может подвергаться произвольному или незаконному вмешательству на неприкосновенность его жилища или тайну его корреспонденции или незаконным посягательствам на честь и репутацию»[1]. К слову, в Европейском союзе действуют и положения, регулирующие обеспечение защиты персональных данных.

Безусловно, Российская Федерация не отстает от других стран, так же принимает непосредственное участие в информационных правоотношениях и на законодательном уровне старается обеспечить информационную безопасность.

Созыкин А.С. АКТУАЛЬНЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ // Студенческий форум: электрон. научн. журн. 2021. № 40(176). URL: https://nauchforum.ru/journal/stud/176/101060 (дата обращения: 08.09.2025).

Так, к примеру, частью 2 статьи 23 Конституции Российской Федерации[2] закреплено право каждого гражданина на тайну переписки, почтовых, телеграфных и иных сообщений.

А частью 1 статьи 24 Конституции Российской Федерации[2] запрещен сбор, хранение и распространение информации о частной жизни лица без его согласия. В то же время одним из принципов гражданского права является недопустимость произвольного вмешательства кого-либо в частные дела граждан.

Кроме того, в Российской Федерации приняты и такие правовые акты, как Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»[4], Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»[5], Требования к защите персональных данных при их обработке в информационных системах персональных данных, утвержденные постановлением Правительства Российской Федерации от 01.11.2012 № 1119[7] и другие.

Однако сказать о том, что безопасность информационных данных в Российской Федерации обеспечена на 100% невозможно.

Для того чтобы ответить на вопрос почему так происходит, для начала следует рассмотреть причины такого явления как «утечка информации».

Изучив научную статью Баранова Р.Г. и Гневанова М.В.[10], можно прийти к выводу, что причинами утечек могут являться: человеческий компонент, организационно-правовое обеспечение и технический компонент.

Особое внимание авторы работы уделяют именно человеческому компоненту и это небезосновательно, так как информационная безопасность это больше социальное, нежели техническое явление.

Человек, в данном случае субъект, имеющий доступ к информации, несет наибольшую угрозу безопасности информации в силу того, что он может применить незаконно полученную информацию не по назначению и это несравнимо с последствиями какого-то простого сбоя в компьютерной программе и потерей данных.

Выявить человека укравшего и распространившего данные крайне сложно, ведь сегодня персональные данные хранятся почти везде: в социальных сетях, в финансовых организациях, в медицинских организациях, в местах работы.

В свою очередь кража данных может повлечь за собой существенные финансовые, юридические и репутационные последствия.

По сравнению с последствиями ответственность за подобные деяния крайне мала. Кроме статьи 137 Уголовного Кодекса Российской Федерации[3], на основании которой происходит привлечение к ответственности за похищение и распространение персональных данных, меры ответственности могут быть сформулированы в соответствии со специальными положениями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных»[5], который отсылает к возможностям других нормативных актов для привлечения к ответственности. Административных мер при этом законодатель для нарушителей частной жизни, к сожалению, не предусмотрел.

Так, за незаконный сбор личной информации о частной жизни человека преступник может понести наказание в виде: штрафа в размере до двухсот тысяч рублей; штрафа в размере своей заработной платы (иного дохода) за период до восемнадцати месяцев; обязательных работ от ста двадцати до ста восьмидесяти часов; исправительных работ до одного года; ареста до четырех месяцев; лишения свободы до двух лет с лишением права занимать определенные должности (заниматься определенной деятельностью) на срок до трех лет.

Но следует помнить, что понести наказание за преступление может лишь то лицо, вина которого будет доказана правоохранительными органами.

И вот здесь-то как раз и начинаются проблемы - сотрудников полиции не направляют на курсы повышения квалификации по расследованию данной категории преступлений, методики расследования данных уголовных дел устарели, а новые методики не разрабатываются.

В итоге получается, что наше законодательство и методики расследования отдельных видов преступлений отстают от реальности.

Искоренить проблему за один день или даже за один год не получится, да и вообще, следует сказать, что проблема обеспечения информационной безопасности будет существовать всегда и во всех странах, так как новые способы завладения конфиденциальной информацией появляются ежедневно, однако, можно развить систему обеспечивающую безопасность информации с помощью межгосударственного партнерства, а также вложения достаточного уровня инвестиций в область исследования и обучения.

Все описанное ранее лишь позволяет решить проблему последствий нарушений информационной безопасности, а для того, чтобы не допустить утечки собственных данных правильным будет следовать нескольким принципам:

1. В социальных сетях следует устанавливать сложные пароли, сочетающие в себе числа, буквы и специальные символы;

2. Не стоит писать лишнее в социальных сетях, не следует отправлять фотографии своих документов посредством социальных сетей;

3. Следует регулярно проверять банковские счета и обязательно проверять выписки и статистику по всем операциям;

4. Не следует отвечать на звонки с незнакомых номеров, а если вышло ответить, то нельзя сообщать данные о себе, о своей банковской карте, нельзя отвечать на вопросы прямо;

5. Заполняя анкеты в различных организациях (по типу бутиков одежды, продуктовых магазинов или магазинов косметики), не следует указывать свои настоящие данные.

Проблема и правда серьезная еще ведь и в силу того, что в Российской Федерации вопрос об информационной безопасности рассматривается как один из аспектов военного обеспечения национальной безопасности страны. Как утверждает Дубень А.К., «в наше время появилась тенденция смещения военных опасностей и угроз в информационное пространство»[11].

И действительно, с этим сложно поспорить, так как распространились такие явления, как разведывательная деятельность иностранных государств на территории Российской Федерации и информационно-техническое воздействие, в том числе кибероружие. На сегодняшний день правовое регулирование информационной безопасности в сфере обороны осуществляется совокупностью норм законодательства Российской Федерации в основе которых лежат нормативно-правовые акты стратегического значения, к примеру: Стратегия национальной безопасности Российской Федерации[8], Военная доктрина Российской Федерации[6], Доктрина информационной безопасности Российской Федерации[7].

Однако для решения данной проблемы также не обойтись без согласованной системы международной информационной безопасности.

А пока данная система будет развиваться, внутри государства можно предпринять следующие меры по обеспечению информационной безопасности:

- увеличить возможность обеспечения кибербезопасности;

- усилить возможности по предотвращению и контролю киберпреступных деяний;

- обеспечить защиту национальной сетевой и информационной безопасности.

Таким образом, обеспечение информационной безопасности – это самостоятельный вид как внутригосударственной, так и внешнегосударственной проблемы. Проблема обеспечение информационной безопасности касается как отдельной личности, так и государства в целом. Информационная безопасность, обеспеченная должным образом, способствует повышению внутренней стабильности страны, а также наращиванию потенциала, необходимого для усиления ее роли в качестве одного из влиятельных центров современного мира.

Список литературы:

1. Международный пакт о гражданских и политических правах от 16.12.1966 принят Резолюцией 2200 (XXI) на 1496-ом пленарном заседании Генеральной Ассамблеи ООН.- Доступ из справочно-правовой системы «Консультант Плюс».- Режим доступа: по подписке.

2. Конституция Российской Федерации (принята всенародным голосованием 12.12.1993) (с учетом поправок, внесенных Законами РФ о поправках к Конституции РФ от 30.12.2008 N 6-ФКЗ, от 30.12.2008 № 7-ФКЗ, от 05.02.2014 № 2-ФКЗ, от 01.07.2020 № 11-ФКЗ) // Собрание законодательства РФ, 01.07.2020, № 31, ст. 4398.

3. Уголовный кодекс Российской Федерации от 13.06.1996 г. № 63-ФЗ по сост. на 01.07.2021 г. // Собрание законодательства РФ, 17.06.1996, № 25, ст. 2954.

4. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. № 149-ФЗ по сост. на 02.07.2021 г. // 31.07.2006, № 31 (часть I), ст. 3448.

5. О персональных данных: Федеральный закон от 27.07.2006 № 152-ФЗ по сост. на 02.07.2021 // Собрание законодательства РФ 31.07.2006, № 31 (часть I), ст. 3451.

6. Военная доктрина Российской Федерации от 25.12.2014 № Пр-2976.- Доступ из справочно-правовой системы «Консультант Плюс».- Режим доступа: по подписке.

7. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 г. № 646 по сост. на 05.12.2016 г. // Собрание законодательства РФ, 12.12.2016, № 50, ст. 7074.

8. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 г. № 400 по сост. на 02.07.2021 г. // Собрание законодательства РФ, 05.07.2021, № 27 (часть II), ст. 5351.

9. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных: Постановление Правительства РФ от 01.11.2012 № 1119 по сост. на 01.11.2012 г. // Собрание законодательства РФ 05.11.2012, № 45, ст. 6257.

10. Баранов Р.Г., Гневанов М.В. Проблемы обеспечения информационной безопасности государственных баз данных и автоматизированных информационных систем Российской Федерации // Московский экономический журнал. 2021. №2. URL: https://cyberleninka.ru/article/n/problemy-obespecheniya-informatsionnoy-bezopasnosti-gosudarstvennyh-baz-dannyh-i-avtomatizirovannyh-informatsionnyh-sistem (дата обращения: 22.11.2021).

11. Дубень А.К. Информационная безопасность как составная часть национальной безопасности Российской Федерации // The Scientific Heritage. 2021. №74-4. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-kak-sostavnaya-chast-natsionalnoy-bezopasnosti-rossiyskoy-federatsii-2 (дата обращения: 22.11.2021).