УДК 008.02

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СЕТИ ИНТЕРНЕТ: СОВРЕМЕННЫЕ ВЫЗОВЫ

Фейзиева С. Ф.

студентка 4-го курса
департамента политологии и социологии,
Уральский федеральный университет
г. Екатеринбург, Россия
feizieva96@mail.ru

THREATS OF INFORMATION SECURITY IN THE INTERNET: CURRENT CHALLENGES

Fejzieva S

student of the 4th year
Department of Political Science and Sociology,
Ural Federal University
Yekaterinburg, Russia
feizieva96@mail.ru

Аннотация

В статье рассматриваются основные угрозы информационной безопасности в сети Интернет. Автор проводит классификацию актуальных вызовов, сопровождающих Интернет-активность современных пользователей, более подробно останавливаясь на угрозах техническому обеспечению и угрозах информационного и психологического характера.

Annotation

The article deals with the main threats to information security in the Internet. The author classifies the actual challenges that accompany the Internet activity of modern users, detailing the threats to technical support and threats of information and psychological nature.

Ключевые слова*:* Интернет, информационная безопасность, кибербезопасность, угрозы информационной безопасности.

Keywords: Internet, information security, cybersecurity, threats to information security

Современное развитие социальной жизни человека на рубеже XX-XXI в. связано с нарастающими оборотами информатизации и компьютеризации всех областей науки. Основным продуктом деятельности становится информация, а самой деятельностью человека ее хранение, обработка и распространение.

В результате глобальной информатизации, Интернет стал общедоступной коммуникативной сетью, которая вышла на авансцену социального, культурного и политического развития общества. Революционное развитие Интернета влекло за собой столь же быстрое развитие угроз, возникающих из-за сложностей повсеместного контроля сети. С каждым днем возрастает необходимость сохранения баланса между свободным распространением информации и обеспечением безопасности личности и общества в целом.

Общеизвестная сеть Интернет берет свое начало в 70-х годах прошлого века. В 1969 г. Министерство обороны США и Агентство передовых исследовательских проектов (ARPA) приняли решение о создании надежной системы информации на случай военных действий и необходимости быстрого контроля и передачи информации. Первая компьютерная сеть под названием Advanced Research Projects Agency Network (ARPANET) объединяла четыре крупнейших научных университета Америки и использовалась для исследований, финансируемых Министерском обороны США. В 1973 году к сети были подключены иностранные организации из Великобритании и Норвегии и сеть стала международной [1].

Повсеместное развитие сеть получила в 90-х, а уже в начале 2000-х годов насчитывалась около 400 миллионов пользователей Интернета по

всему миру (6% население планеты) [2]. Информационная революция позволила без труда получать доступ и делиться информацией вне зависимости физических границ пространства и времени. Одним словом, было создано «виртуальное пространство», живущее по своим собственным законам. В таких условиях у пользователей сети появилась возможность мгновенно получать и передавать информацию в любую точку земного шара.

Влияние информационных технологий и информатизации неизбежно. И на данный момент информация по праву признается стратегическим ресурсом любого государства. В этой связи возникают различные опасности, связанные с хранением и распространением информации. В правотворческой отрасли выделилась отдельная сфера информационного права, которая стоит «на страже» информационной безопасности общества. Под ней понимается «состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [3].

Целью данной статьи является классификация современных угроз информационной безопасности в сети Интернет и поиск возможных путей реагирования на них.

Понятие «угрозы» описано в Стратегии национальной безопасности Российской Федерации до 2020 года. «Угроза – это прямая или косвенная возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию Российской Федерации, обороне и безопасности государства» [4]. Угроза информационной безопасности в сети Интернет может обозначатся как потенциальная возможность причинения ущерба жизненно-важным интересам личности, общества и государства с использованием информационно-коммуникативных средств сети Интернет.

Важное место в системе информационной безопасности занимает классификация возникающих угроз, с которыми может столкнуться каждый

пользователь сети. С одной стороны, Интернет — это «всемирная коммуникационная система, состоящая из сотен небольших компьютерных сетей, связанных между собой телефонными сетями» [5], а с другой стороны Интернет – это информационная среда, основной задачей которой является распространение информации. В связи с этим угрозы можно разделить на два вида:

1) угрозы нарушения конфиденциальности, доступности и целостности информации;

2) угрозы нарушения требований к содержательной части информации [6].

Первый вид угроз относится к технической стороне использования Интернета, - это повреждения программного обеспечения компьютера, хранящейся на нем информации, нарушение ее конфиденциальности или хищение персональной информации [7]. Отдельно выделают вирусные атаки, которые наносят вред и технической и информационной стороне работы компьютера.

Второй вид угроз включает в себя опасности информационного и психологического характера, возникающие вследствие доступа к незаконному контенту. Законодательством Российский Федерации запрещено распространение порнографии, экстремистских материалов, фашисткой символики, информации оскорбляющей достоинство личности и материалов, пропагандирующих употребление наркотических веществ. Особое внимание уделяется защите детей от противоправной информации, в связи с чем был разработан закон «*О защите детей* от *информации*, причиняющей вред их здоровью и развитию».

Помимо вышеперечисленных угроз, можно выделить такие как: траля (кибербуллинг), сексуальные домогательства (груминг), пересылка сообщений интимного характера (секстинг). Чаще всего эти действия распространяются в социальных сетях, где происходит непосредственное общение пользователей. На таких платформах имеет место быть

целенаправленное создание аккаунтов несуществующих в реальности пользователей с целью того или иного психологического давления.

Информационная безопасность, будучи отраслью национальной безопасности государства, обращает внимание и на более глобальные виды угроз – политические. К ним относят: информационные войны, кибервойны, электронную разведку, компрометацию государственной тайны, атаки на информационные системы важных оборонных, транспортных и промышленных объектов, неполного информирования и дезинформации руководителей крупных учреждений [8].

Поимо этого, не стоит забывать о существовании, так называемого, «теневого интернета», который содержит закрытые сети для общения узкой группы лиц, обычно террористических группировок. Их главным козырем становится молниеносность распространения информации и новые возможности дистанционного управления террористическими актами.

Как можно заметить, классификация угроз информационной безопасности в сети Интернет довольно обширна. Невозможно предугадать чего стоит остерегаться пользователям в ближайшем будущем. Государство, как субъект обеспечения безопасности, на законодательном уровне закрепляет принципы функционирования Интернета на территории Российской Федерации, а также устанавливает надзор за действиями граждан в сети.

Но не все противоправные действия могут быть отслежены. Интернет обладает такими свойствами, которые не позволяют осуществлять всеобъемлющий надзор. Такими свойствами являются: экстерриториальность, сетевая структура, порождающая децентрализованный характер и его безграничность. В таких условиях законодательство одной страны не в силах обеспечить необходимую безопасность пользователям. Одним из путей совершенствования системы информационной безопасности видится синергия мировой правовой системы, права отдельно взятой страны и самоконтроль самих пользователей.

Только во взаимодействии этих трех уровней можно добиться эффективной работы системы информационной безопасности в сети Интернет.

Список литературы

1. Гришанова Е. М., Артамонова Я. С., Чиликин И. А. Информационная безопасность и информационные коммуникации // T-Comm. 2012. №12. С.14-16
2. The world in 2015 // International Communication Union URL: https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf (дата обращения: 23.02.2018).
3. Доктрина информационной безопасности Российской Федерации // Российская газета. – 2000.
4. Указ Президента Российской Федерации от 12 мая 2009 года № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года» // Российская газета. 2009.
5. Интернет // Научно-технический словарь: Академик URL: https://dic.academic.ru/dic.nsf/ntes/1799 (дата обращения: 23.02.2018).
6. Напханенко Екатерина Олеговна Понятие и классификация угроз информационной безопасности в сети Интернет // ЮП. 2011. №4.
7. Солдатова Г. У. Цифровая компетентность подростков и родителей. Результаты всероссийского исследования / Г. У. Солдатова, Т. А. Нестик, Е. И. Рассказова, Е. Ю. Зотова. — М.: Фонд Развития Интернет, 2013. С. - 95-96.
8. Алиева М.Ф. Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного университета. Серия 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. 2012. №4. С. 104.