# ОБ ИННОВАЦИОННЫХ МЕТОДАХ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ИНТЕРНЕТЕ

***Приходовский М.А.,*** *кандидат физико-математических наук, доцент Томского государственного университета систем управления и радиоэлектроники.*
prihod1@yandex.ru

Актуальность проблемы информационной безопасности с каждым годом будет возрастать, так как компьютеры всё больше используются в работе жизненно важных систем: в диспетчерских службах аэропортов, в управлении энергетикой, ядерными и химическими производствами. Серьёзную угрозу могут представлять вирусы, распространяемые через электронную почту и другими способами. Вирусные программы в будущем могут вызвать крупный сбой в системах жизнеобеспечения и техногенные катастрофы.

Проблемы, связанные с информационной безопасностью, можно условно разделить на 2 глобальных класса вопросов:

а) противодействие незаконному получению информации;

б) противодействие незаконной передаче информации.

К первому относится борьба против взлома баз данных и промышленного шпионажа; кодирование информации при передаче по каналам связи. Ко второму направлению – борьба с распространением вирусов, вызывающих компьютерные сбои, а также противодействие возможному влиянию через компьютерные сети на работу жизненно важных систем. В свою очередь, противодействие рассылке вирусов и спама возможно на трёх этапах: при отправке, прохождении по сетям и получении. Второе и третье направление активно развивается специалистами по информационной безопасности. Создаются антивирусные программы. Но это решает проблему лишь частично, так как меры защиты только на стадии входящей почты не могут быть абсолютно эффективными. Возрастает криминализация интернета и количество преступлений в сфере высоких

технологий. Сейчас почтовый ящик может создать кто угодно на фиктивное имя, есть и программы автоматической регистрации. Возможность остаться неизвестным – вот самое важное, чем пользуются нарушители. Принцип работы электронной почты, при котором регистрация ящика происходит через интернет, уже устарел.

Наиболее эффективной мерой будет являться борьба с вирусами, спамом и угрозами по электронной почте на этапе отправления, то есть предотвращение появления источника. Для этого не нужны ограничения и цензура, самой действенной мерой станет повышение ответственности пользователей интернета вследствие введения системы идентификации с помощью персональных чипов. Предлагаемые далее в статье меры делают доступ в интернет похожими на доступ к сети сотовой и прочей телефонной связи и сильно ограничивают возможность распространения спама и вирусов.

**1. Электронная почта – по договору с почтовой компанией.**

Пользователь для получения имени почтового ящика подписывает бланк договора на оказание услуг электронной почтовой связи с фирмой Mail, Yandex или другими. В договоре указываются персональные данные пользователя. Всё это никаким образом не ограничивает свободу переписки. Можно завести себе много адресов, в разных почтовых системах. Например, для сравнения, договор на оказание услуг сотовой связи заключается в офисе сотовой компании с предъявлением паспорта. Но человек имеет свободу выбора подключиться к той или иной сети, и даже получить две и более SIM-карт, подключаясь с разными тарифными планами. Почтовые службы скорее всего будут заинтересованы в упорядочении работы своих клиентов указанным способом, так как это, в перспективе, сильно уменьшает возможности спамеров. Полностью исчезнет такое понятие, как автоматические регистрации, анонимность электронной почты.

**2. Провайдерские чип-карты.**

Можно персонифицировать подключение к компьютерной сети интернет – при запуске Internet Explorer программа потребует присоединить к

порту USB персональное устройство, выдаваемое компанией-провайдером, и ввести PIN-код. Данное микро-устройство может по виду напоминать FLASH, а по действию аналогичного SIM-карте сотового телефона или банковской пластиковой магнитной карте. Такой магнитный контроллер осуществляет идентификацию не по IP-адресу, а по персональному номеру карты, договор на которую составляется либо в офисах компьютерных компаний, либо в почтовых отделениях. Это может исключить компьютерные преступления на начальной стадии. В настоящее время IP-адрес ассоциирован с компьютером, а не с личностью, что не всегда позволяет найти человека, совершающего незаконные действия через интернет, особенно если они предприняты из компьютерного класса свободного доступа, где у всех машин один и тот же внешний IP-адрес. Даже если известно, с какой ЭВМ предпринимались действия, не всегда возможно установить личность злоумышленника, который работал за данным компьютером в тот момент времени. IP-адрес аналогичен всего лишь номеру IMEI сотового телефона. Однако любой абонент сотовой сети отождествляется с номером SIM-карты, то есть сотовым номером, на который составлен договор, где указаны персональные данные абонента. Система идентификации с самого начала применялась в телефонной связи. Подобная технология может помочь в борьбе против криминализации интернета. Технические трудности при создании такой системы идентификации легко преодолимы.

Персонификация доступа сначала к почте, а затем и в компьютерные сети, может стать наиболее эффективным способом борьбы с нарушениями в сфере высоких технологий.

СПИСОК ЛИТЕРАТУРЫ

[1] Приходовский М.А. «Информационная безопасность и интернет будущего» URL: www.inauka.ru/blogs/article64754.html

[2] URL: www.rocit.ru/public/index.php3?path=prihod2

Библиографическая ссылка на эту статью:
Приходовский М.А. Об инновационных методах обеспечения безопасности в интернете // Естественные и технические науки. 2006. № 4. С. 246-247