

Шарыпова Т.Н.,

кандидат экономических наук

доцент кафедры информационных технологий и защиты информации

Ростовский государственный экономический университет «РИНХ»

Россия, г. Ростов-на-Дону

Малыгин Е.А.,

студент 1 курс, юридический факультет

Ростовский государственный экономический университет «РИНХ» Россия,

г. Ростов-на-Дону

ЗАЩИТА ИНФОРМАЦИИ В INTERNET

Аннотация: в данной статье рассматривается проблема незащищенности информации в сети Internet, способы ее решения.

Abstract: this article discusses the problem of the vulnerability of information on the Internet, how to solve it.

Ключевые слова: интернет, компьютерная сеть, безопасность данных, незащищённость ресурсов, информация.

Keywords: Internet, network, computer, data security, resource insecurity, information.

Internet - всемирная компьютерная сеть, которая охватывает весь мир. На данный момент Internet включает в себя примерно 3,3 млрд. пользователей в большинстве стран мира. В сеть Internet входит множество локальных и глобальных сетей, которые относятся ко многим компаниям и организациям, которые сплетены между собой каналами связи. Эту компьютерную сеть можно представить небольшими сетями различной величины, которые тесно взаимодействуют друг с другом.

Вначале она создавалась как корпоративная сеть, но в данный момент времени, благодаря единому стоку протоколов TCP/IP и единому адресному пространству, объединяет корпоративные и ведомственные сети, которые сейчас являются сетями с ограниченным доступом, а также обыкновенных пользователей, имеющих возможность получать прямой доступ в сеть Internet со своих домашних ПК [1].

Internet привлекает потенциальных пользователей своей быстротой, гибкостью, дешевой глобальной связью, удобством для проведения совместных работ, доступностью программ и уникальной, универсальной базой данных сетей. При низкой стоимости услуг, практически каждый человек способен получить доступ к коммерческим и некоммерческим информационным службам многих стран. В архивах открытого доступа сети можно найти информацию почти обо всех сферах человеческой деятельности, начиная с научных открытий современности и заканчивая метеорологическими прогнозами в городах по всему миру.

Чем легче получить доступ в сеть, тем сложнее сохранить её информационную безопасность. К примеру, пользователь может даже не подозревать, что у него были скопированы файлы и программы. Не говоря о факте возможности их порчи, утраты или же замены. Платой за пользование сетью является всеобщее понижение информационной безопасности.

Обеспечение безопасности данных является одной из самых главных проблем в сетевом мире. Всё чаще и чаще появляются данные о том, как злоумышленники, использующие все более изощрённые способы и приемы, проникают в чужие базы данных и получают доступ в архивы коммерческих данных. Разумеется, все это уменьшает популярность Internet в деловых кругах. Одна только мысль о том, что есть шанс заполучить доступ к архивам коммерческих данных, заставляет руководство корпораций отказываться от использования открытых информационных систем. Специалисты утверждают, что подобные опасения не подкреплены доказательствами, так как у корпораций,

владеющими доступом и к открытым, и частным сетям, практически одинаковы шансы стать жертвами компьютерных атак.[2]

Проблема безопасности ставит выбор между защищённостью и доступностью своего имущества, возможность свободного пользования им. Это справедливо и в отношении информации. К примеру, база данных, которая содержит полную аутентификацию сведений, абсолютно полностью защищена от проникновений лишь тогда, когда находится на дисках, изъятых с компьютера и убранных в защищённое пространство. Стоит установить диски в компьютер, как сразу возникает несколько вариантов каналов, по которым злоумышленник способен быстро проникнуть и получить доступ к данным. Таким образом, информация либо недоступна для всех пользователей, либо недостаточно защищена. В области информации встаёт ещё один выбор: между защищённостью системы и ее открытостью. Здесь имеет место быть даже не вывод, а баланс, так как система, которая не обладает свойством открытости, не может быть использована [4].

Платой за пользование Internet являются следующие информационные угрозы:

- создание внешних угроз на корпоративную сеть;
- несанкционированный доступ к сети компаний со стороны рабочих станций, удаленных и передающих серверов, использованных в сети Internet;
- утрата информации в каналах связи Internet в результате заражения вирусными программами, безалаберности сотрудников, отказа канала связи, стихийных бедствий;
- несанкционированный программно-аппаратный доступ к информации, включенной в канал связи Internet;
- несанкционированное использование доступа к информации через электромагнитные излучения каналов связи и средств передачи информации Internet;
- несанкционированное использование доступа информации, размещенной на удаленных серверах Internet;

- сбор и обзор сетевой информации в интересах третьих лиц;
- переизбыток ненужной и вирусной информации в системе.

Таким образом, если ПК или корпоративная сеть считаются носителями важной информации, нужно серьезно подумать перед тем, как подключить её к сети, а перед использованием последующих советов выполнить все рекомендации по средствам защиты; совершить доскональный отбор и изъятие личной информации из подключаемой сети или ПК. Также важно посоветоваться с профессиональными сотрудниками, которые занимаются информационной безопасностью, и исполнить нижеперечисленные рекомендации [3].

Выделяют следующие способы защиты:

- при работе в сети Internet на первое место становится "межсетевой экран" или защитник Windows. Защитник Windows - неотъемлемая часть защиты системы. Защитник Windows даёт возможность значительно уменьшить количество эффективных внешних угроз на корпоративную сеть или ПК, несанкционированный доступ к сети организации со стороны рабочих станций, удаленных и передающих серверов, включенных в сеть Internet, уменьшить вероятность сбора и обзор сетевой информации в интересах третьих лиц, блокировать доступ бесполезной и вирусной информации в систему;
- использование VPN технологии, систем алгоритмов, криптографирования (электронной подписи, сжатия с паролем, шифрования), даёт возможность уменьшить утраты от непредвиденного доступа к личной информации, которая находится в канале связи Internet, данный доступ к информации через электромагнитные излучения каналов связи и средств передачи информации Internet, а также доступа к информации, поставленной на удаленных и передающих серверах Internet, сбор и обзор информации в интересах третьих лиц;
- повторение канала Internet, и сокращение информации дает возможность повысить протект системы в случае отказа или перегрузки канала связи и в случае стихийных катастроф;

- использование антивирусных программ, считается необходимым условием при подключении к сети Internet, это позволяет гораздо уменьшить утерю информации в результате проникновения вирусных программ;
- применение автоматических средств для анализа сети на наличие возможной незащищенности в системе протекта и аудита безопасности корпоративных серверов даёт возможность найти источники угроз и на много уменьшить процент гораздо эффективных атак на корпоративную сеть или ПК;
- применение программы Proxu и скрытных серверов даёт возможность оставаться условно анонимным при действиях в сети Internet и понизить риск, связанный со сбором и обзором сетевой информации в интересах третьих лиц, потоком ненужной и вирусной информации в систему;
- применение систем ограничения доступа сотрудников к сетевым ресурсам Internet, использование маршрутов и безопасных поставщиков сетевых услуг, краткосрочного канала связи дают возможность уменьшить сбор и обзор сетевой информации в интересах третьих лиц, поток ненужной и вирусной информации в систему [5].

ИСПОЛЬЗУЕМЫЕ ИСТОЧНИКИ

1. Гилстер П. Браун С. “Мозаика” и “Всемирная паутина” для доступа к Internet: Пер. с
2. Новый навигатор Internet: Пер с англ. -Киев: Диалектика, 1996. - 495 с.
3. Игер Б. Работа в Internet / Под ред. А. Тихонова; Пер. с англ. - М.: БИНОМ, 1996. - 313 с.
4. Скляр А.В., Тищенко Е.Н., Шарыпова Т.Н., Ефимова Е.В. Эволюционные вычисления в задаче управления информационными рисками защищенных экономических систем. Экономические науки. 2017. № 148. С. 27-29.
5. Скляр А.В., Тищенко Е.Н., Стрюков М.Б., Шарыпова Т.Н. Управление информационными рисками защищенных экономических систем на

основе анализа нечетких временных рядов. Вопросы экономики и права. 2016.
№ 98. С. 58-60.