пользователей сети массой рекламных писем. С того момента Лоренса Кантера и Марту Сигел принято считать первооткрывателями «спама».

Иногда достаточно всего один раз указать свой электронный адрес в Интернете, чтобы попасть в список к спамерам. Но чтобы защититься от спама, необходимо знать уловки и соблюдать несколько правил:

– Использование нескольких почтовых ящиков.
– Механизм фильтрации почты.
– Антиспамовые программы.
– Ни в коем случае нельзя открывать и запускать файлы, присланные незнакомыми или малознакомыми людьми. Такие письма необходимо удалять сразу. Файл, прикрепляемый к сообщению, может содержать любую вредоносную программу: вирус, макровирус, червь, «троян», шпионскую программу и прочее.

Таким образом, E-mail является отличным средством общения людей. Однако, при работе с электронной почтой не стоит также забывать про безопасность и следовать правилам которые помогут избежать различные угрозы.

Программные закладки и методы защиты от них

Свирская М.А., Толстая М.И.
Научный руководитель: Ковалькова И.А.
Белорусский национальный технический университет

В настоящий момент информация является одной из важнейших ценностей человеческого общества. Стоимость информации значительно превосходит стоимость информационных систем её обработки и хранения. В связи с этим возникает проблема защищённости компьютерных систем от утечки информации по каналам несанкционированного доступа. Наиболее удобным способом проникновения в систему для злоумышленника является программная закладка.

Программная закладка – это программа или фрагмент программы, который скрытно внедряется в защищённую систему и позволяет преступнику, внедрившему его, осуществлять в дальнейшем несанкционированный доступ к тем или иным ресурсам защищённой системы. Существует два вида программных закладок: алгоритмические и программные.

Алгоритмическая закладка – это преднамеренное скрытое искажение части алгоритма программы, в результате чего возможно появление у программного компонента функций, не предусмотренных спецификацией

и выполняющихся при определённых условиях протекания вычислительного процесса.

Программная закладка – это внесённые в программное обеспечение функциональные объекты, которые при определённых условиях (входных данных) инициируют выполнение не описанных в документации функций, позволяющих осуществлять несанкционированные воздействия на информацию.

Ими могут выполняться следующие действия:

1) Копирование информации пользователя компьютерной системы(паролей, криптографических ключей, кодов доступа, конфиденциальных электронных документов), находящейся в оперативной или внешней памяти этой системы, либо в памяти другой компьютерной системы, подключённой к ней через локальную или глобальную компьютерную сеть.

2) Изменение алгоритмов функционирования системных, прикладных и служебных программ (например, внесение изменений в программу разграничения доступа может привести к тому, что она разрешит вход в систему всем без исключения пользователям вне зависимости от правильности введённого пароля).

3) Навязывание определённых режимов работы (например, блокирование записи на диск при удалениинформации, при этом информация, которую требуется удалить, не уничтожается и может быть впоследствии скопирована хакером).

Изменения в функционировании, которые могут наблюдаться при работе программной закладки в системе могут быть следующие:

– снижение быстродействия вычислительной системы;

– частичное или полное блокирование работы системы;

– имитация физических (аппаратных) сбоев работы вычислительных средств и периферийных устройств;

– переадресация сообщений;

– обход программно-аппаратных средств криптографического преобразования информации;

– обеспечение доступа в систему с несанкционированных устройств.

Одним из возможных методов защиты от программных закладок является использование принципа минимальных полномочий, в соответствии с которым каждому субъекту (процессу или пользователю) всегда предоставляются в системе минимальные права.

Для обнаружения присутствия в системе программной закладки могут применяться следующие способы:

1) Просмотр списка активных процессов с помощью диспетчера задач операционной системы;

2) Просмотр состояния IP-портов с помощью системной программы netstat;

3) Просмотр разделов реестра для обнаружения дополнительно установленных программ, которые автоматически выполняются при загрузке операционной системы;

4) Просмотр файла аудита для поиска попыток доступа неизвестных процессов к критичным объектам компьютерной системы или объектам с конфиденциальной информацией;

5) Контроль обращений процессов к объектам файловой системы, разделам реестра и используемым сетевыми программами портам (например, с помощью известных программ FileMon, RegMon и PortMon) и др.

Некоторые антивирусные программы (сканеры и мониторы) могут обнаруживать инсталляторы закладок и сами закладки.

Наиболее эффективным методом защиты от программных закладок является использование организационных мер, к которым можно отнести следующие:

1) Минимизация времени работы в компьютерной системе с полномочиями администратора;

2) Создание специальной учётной записи пользователя компьютерной системы для выхода в сеть Интернет с минимальными полномочиями (запуск обозревателя и сохранение файлов в специальной папке);

3) Аккуратное использование почтовых и офисных программ привилегированными пользователями (например, запрет доступа администратора к отдельным папкам и файлам).

Эффективным методом защиты от вредоносных программ является создание изолированной программной среды, обладающей следующими свойствами:

1) На компьютере с проверенной BIOS установлена проверенная операционная система;

2) Достоверно установлена целостность модулей операционной системы и BIOS для данного сеанса работы пользователя;

3) Исключён запуск любых программ в данной программно-аппаратной среде, кроме проверенных;

4) Исключён запуск проверенных программ вне проверенной среды их выполнения (т.е. в обход контролируемых проверенной средой событий).

В итоге, можно сделать вывод, что внедрение программных закладок может произойти случайно через сеть или носители информации. Однако программная закладка может быть внедрена в любой программе изначально, ещё на стадии создания программы. Выявить такие закладкипрактически невозможно. Следовательно, для уменьшения риска

и угроз, нужно устанавливать доверенные программы и пользоваться рядом правил и мер предосторожности.

Литература

1. Романец Ю., Тимофеев П., Шаньгин В. «Защита информации в компьютерных системах и сетях». – М.: Радио и связь, 2001 – 376 с.
2. Казарин О.В. «Теория и практика защиты программ». – М.: МГУЛ, 2004. – 450 с.
3. https://shkolazhizni.ru/law/articles/36906/
4. http://kiev-security.org.ua/box/12/79.shtml
5. http://infoprotect.net/protect_pk/programmnyie_zakladki
6. http://ruseti.ru/book8/2/Index1.htm

Геоинформационные системы и их перспективы применения в сфере таможенного дела

Дедюля А.А.
Научный руководитель: Галай Т.А.
Белорусский национальный технический университет

Таможенное дело – актуальная для развития сфера практически в любой стране, в особенности это касается Беларуси, которая находится в центре Европы и является своеобразным мостом между западным и восточным экономико-политическими блоками. В период постоянного увеличения темпов роста торговли перед Беларусью стоит задача по увеличению пропускной способности через таможенную границу. Появление новых видов контрабанды, в свою очередь, обуславливает необходимость усовершенствования контроля пропускаемых товаров.Эти и другие задачи могут быть реализованы с помощью внедрения геоинформационных систем (ГИС) в таможенное дело.

Основными компонентами ГИС являются: компьютер и его периферия, программное обеспечение ГИС, данные (в том числе геопространственные) и соответствующие специалисты [1].

На ГИС возлагается выполнение ряда функций:автоматизированного картографирования; пространственного анализа; управления данными.

Одними из важных задач, поставленных перед ГИС, являются визуализация и упрощение работы с информацией.Для достижения этих задач в геоинформационных системах географическая информация представлена и храниться послойно. Схематично это изображено на рисунке 1 [2].