системы, а контроль деятельности(аудит) уполномоченного пользователя – администратор безопасности информационных систем.

Информационные системы и информационные технологии широко используются таможенными органами в целях обеспечения выполнения возложенных на них функций, в том числе обмена информацией с государственными органами, оказания государственных услуг участникам внешнеэкономической деятельности по предоставлению информации в электронном виде.На таможнях Республики Беларусь широко применяются следующие системные обеспечения: АС «Декларант», АС «Мониторинг-ВПТО», АС «СЭЗ», АРМ «ПТО», АРМ «БТС: Специалист», ПМ «Таможенный перевозчик». Следовательно, выполнение описанных способов и мер защиты информации позволит повысить уровень защищённости информации, циркулирующей в таможенных подразделениях до требуемого уровня безопасности.

Безопасное использование электронной почты(e-mail), выбор почтового клиента. Защита от спама

Маринич А. А.
Научный руководитель: КовальковаИ.А.
Белорусский национальный технический университет

Электронная почта (***E-mail***)– система, которая делает возможным передачу сообщений через глобальные и локальные сети компьютеров, в том числе через Интернет.

Электронная почта является важнейшим средством коммуникации, распределения информации, она решает одну из важнейших на настоящий момент задач – формирует единое информационное пространство, которая упрощает обмен информацией между людьми, подразделениями одной компании и различными организациями.Работа электронной почты, не зависит от разницы в часовых поясах, поэтому можно вести переписку по электронной почте с адресатом, который находится на другом конце света.

Для создания и получения сообщений электронной почты применяются специальные почтовые программы.*Почтовые клиенты* – это программы, с помощью которых пользователь может принимать и отправлять почту. Таких программ существует достаточно много, но принцип работы у всех одинаковый. Из множества программ электронной почты, работающих под управлением Windows, можно выделить:

- OutlookExpress;
- офисное приложение Microsoft Outlook;
- компоненты электронной почты в составе программ-браузеров;

– The Bat молдавскойкомпании RIT Research Labs;
– Mail, HotMail, Hotbox
– Opera Mail (M2);
– Mozilla Mail организации MozillaFoundation, новое название SeaMonkey;
– Eudora Mail компании Qualcornm (одна из первых e-mail программ)

Почти все эти программы выполняют следующие функции:
– подготовку текста сообщения;
– отсылку и приём корреспонденции;
– чтение и сохранение корреспонденции;
– удаление сообщений;
– ввод адреса (адресов) корреспондента;
– включение в создаваемые сообщения вложений (текстовых, графических файлов, аудио- и видеофайлов);
– вставку в сообщение электронной подписи или визитной карточки отправителя;
– ведение электронной адресной книги;
– комментирование и пересылку полученной корреспонденции другим абонентам;
– поиск нужной корреспонденции по заданным критериям;
– импорт других файлов;
– отложенную отправку почты;
– рассылку корреспонденции по нескольким адресам;
– периодическую проверку новой почты;
– управление модемом для установления IP-соединения;
– сортировку сообщений по «папкам».

Электронная почта способна заменить собой множество факсов и обычную почтовую доставку, так как по сравнению с другими способами передачи сообщений электронная почта имеет ряд преимуществ:
– оперативность и легкость использования;
– доступность практически в любом месте;
– универсальность форматов писем и вложений;
– дешевизна сервиса;
– надёжность и скорость инфраструктуры доставки;
– использование для обработки электронной почты прикладного специального программного обеспечения.

На сегодняшний день электронные письма используются очень широко и по этой причине они стали средством распространения вирусов, спама ифишинговых атак.

Безопасность электронной почты пользователя часто является уязвимым местом, которым пользуются злоумышленники для получения

доступа к важным данным. Основные риски, связанные с её использованием, возникают из-за имеющихся достоинств. Легкость в использовании и бесконтрольность приводит к утечкам информации, возможность пересылки разных форматов документов – к распространению вирусов и т.д.Доступность электронной почты становится недостатком, если пользователи начинают применять почту для рассылки спама.

Любой из этих рисков может привести к таким серьёзным последствиям как потеря эффективности работы, разглашение конфиденциальной информации, а в некоторых случаях и к юридической ответственности.

К сожалению, надёжного способа защиты электронной почты ещё не существует. Безопасность систем электронной почты можно обеспечить только с помощью комплекса мер.

Обеспечить безопасность работы с электронной почтой поможет соблюдение некоторых следующих простых правил:

– Нельзя запускать программы, полученные по электронной почте.

– Не стоит доверять даже «солидным» адресам, такого типа, как support@mail.ru или webmaster@mail.ru.Почтовые сервера никогда не рассылают программ своим пользователям. Адрес отправителя легко подделать. Многие этим пользуются для рассылки вирусов.

– Никому нельзядаватьсвой пароль.Почтовые сервераникогдане просят пользователей прислать действующий пароль к почтовому ящику.

– Открывая полученные файлы MS Office (Word– .doc, Excel – .xls и т.д.)не разрешайте использование макросов.

– Старайтесь пользоваться самыми свежими почтовыми программами. В новых версиях ошибки, связанные с «лазейками» в безопасности устраняются.

Ещё одна трудность, с которой сталкивается любой пользователь, является борьба со спамом. Было подсчитано, что количество рекламных писем сегодня составляет почти половину от всех получаемых пользователями сообщений. Стоит отметить, что такой способ рекламы не является законным.

Спам – это массовая рассылка не запрошенной адресатами информации. Адресат не имеет возможности отказаться от получения таких сообщений в будущем. Для рассылки, как правило, используются интернет-службы, которые обеспечивают её низкую стоимость и анонимность.

Понятие «почтового спама» появилось на свет благодаря деятельности пары американских адвокатов – Лоренса Кантера и Марты Сигел. В начале 1978 года их компания заполонила немногочисленных на то время

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