УДК 004.49

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ФИНАНСОВО–КРЕДИТНОЙ СФЕРЫ (КЛАССИФИКАЦИЯ ЗЛОВРЕДОВ)

***И.А. Исаева**, 1 курс*
*Научный руководитель – **И.А. Янковский**, к.э.н., доцент*
Полесский государственный университет

Информационные технологии – отрасль, развивающаяся в стремительном темпе. Но с новыми возможностями появляются и новые угрозы. Ежедневно пользователи сталкиваются с многочисленными компьютерными вирусами, поражающими файлы и выводящими систему из строя. Поэтому в настоящее время остро стоит проблема кибератак, с которыми борются по всему миру.

Что касается банковской сферы, то проблема информационной безопасности известна там как нигде лучше. Сегодня ни у одного руководителя организации, предприятия, и уж тем более банка не возникнет сомнений в важности и необходимости защиты информации. Обеспечение секретности электронных документов, сохранение различных видов тайн, предотвращение мошенничества со счетами и вкладами клиентов – всё это напрямую связано со степенью информационной безопасности.

Существуют различные способные нанесения угроз информации. Одним из них является угроза информационным способом. Следует понимать, что в таком случае вред наносится из–за противозаконного сбора и использования, скрытия или искажения информации. Реализация угроз техническими способами представляет собой нарушение технологии обработки информации, а также прослушивание, просмотр, перехват информации с помощью технических средств. Что касается физических способов угроз, то они включают в себя хищение, разрушение, уничтожение носителей информации, а также средств, на которых она хранится. Известен также вид угроз, осуществляемых посредством закупки и поставки устаревшего оборудования предприятию, приводящим к дезорганизации работы[1].

В настоящее время пользователям часто приходится сталкиваться со сбоями работы сети, возникновением проблем из–за проникновения вредоносных программ в компьютер. Ю.Мельников выделяет следующие виды зловредов.

1. "«Лазейки» («Trapdoors»). Они представляют собой точки входа программы, при помощи которых можно получить непосредственное управление некоторыми системными функциями. Организуют лазейки с целью наладить программу и проверить её возможности. Но после процесса настройки программы их надо устранить. Обнаружить такую лазейку можно в результате анализа работы программ, изучая логику их действия.

2. «Логические бомбы» («Logic bombs»). Логическая бомба является компьютерной программой, которая приводит к повреждению файлов или компьютеров. Повреждение варьируется от искажения данных до полного стирания всех файлов или повреждения машины. Логическую бомбу инсталируют во время разработки программы. Она активирует свое действие при условии совпадения времени, даты, кодового слова.

3. «Троянский конь» («Trojan horse»). Троянский конь – программа, которая приводит к неожиданным воздействием к системе. Отличительной характеристикой Троянского коня является то, что пользователь обращается к ней, считая ее полезной. Эти программы обладают возможностью раскрыть, изменить или уничтожить данных или файлы.

4. «Черви» («Worms»). Червяк – программа, которая распространяется в системах и сетях по линии связи. Такие программы похожи на вирусы в том, что они заражают другие программы, а различаются тем, что они не обладают способностью самовоспроизводиться. В отличии от Троянского коня червяк входит в систему без знания пользователя и делает свои копии на рабочих станциях сети.

5. «Бактерии» («Bacterium»). В терминологию вредительских программ вошло понятие «бактерия». Она представляет собой программу, которая делает свои копии, перегружая память и процессор.

6. «Вирусы» («Viruses»). Определения вирусов бывают весьма разнообразными, как и сами вирусы. Утвердилось определение доктора Фредерика Коэна: "Компьютерный вирус представляет собой программу, которая способна заражать другие программы, модифицируя их так, чтобы они включали в себя копию вируса (или его разновидность)"[2].

«Лаборатория Касперского» дает свою классификацию. Кроме вышеперечисленных встретились такие вредоносы как «Руткит», «Бэкдор», «Загрузчик».

«Руткит. В современном мире руткит представляет собой особую часть вредоносных программ, разработанных специально, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения. Это возможно благодаря тесной интеграции руткита с операционной системой.

Бэкдор (средство удаленного администрирования). Бэкдор, или RAT (remote administration tool), – приложение, которое позволяет честному системному администратору или злоумышленнику управлять компьютером на расстоянии. В зависимости от функциональных особенностей конкрентного бэкдора, злоумышленник может установить и запустить на компьютере любое программное обеспечение, брать на себя контроль за компьютером и информацией жертвы.

Загрузчик. Эта вредоносная программа является небольшой частью кода, используемого для дальнейшей загрузки и установки полной версии вредоноса. После того как загрузчик попадает в систему путем сохранения вложения электронного письма или, например, при просмотре зараженной картинки, он соединяется с удаленным сервером и загружает весь вредоносный файл»[3].

Сегодня с области безопасности информационных систем применяются самые разнообразные технологии защиты информации. Однако практика показывает, что только комплекс мероприятий способен помочь в достижении поставленной цели. Различные методы защиты информации должны применяться параллельно. Для решения проблемы защиты информации основными средствами, используемыми для создания механизмов защиты принято считать:

"Технические средства – реализуются в виде электрических, электромеханических электронных устройств.

Программные средства – программы, специально предназначенные для выполнения функций, связанных с защитой информации.

В ходе развития концепции защиты информации специалисты пришли к выводу, что использование какого–либо одного из выше указанных способов защиты, не обеспечивает надежного сохранения информации. Необходим комплексный подход к использованию и развитию всех средств и способов защиты информации"[4].

Беларусь, имея развитую систему банков, нуждается в обеспечении информационной безопасности финансово–кредитной сферы. В 1997 году был создан «Центр банковских технологий». С момента образования основным предметом деятельности является развитие информационных технологий в денежно–кредитной системе Беларуси, в том числе автоматизация деятельности Национального банка Республики Беларусь. В октябре 2013 года стало известно о том, что «Центр банковских технологий» планирует создать в своей структуре подразделение оперативного реагирования для противодействия кибермошенничеству в банковской сфере. Для более полного удовлетворения запросов банковско–финансовой сферы в области информационной безопасности акционеры и руководство ОАО "Центр банковских технологий" решили создать на базе предприятия специальное подразделение оперативного реагирования (CERT–CBT). Новая структура может заработать уже в 2014 году. Ее создание будет идти при научно–технической поддержке со стороны польской компании ComCERT SA.

Таким образом, обеспечение защиты информации является одним из ведущих направлений разработок IT–компаний по всему миру. Значимость и необходимость информационной безопасности стоит на первом месте в организации безопасной работы сети банков и защиты прав и интересов их клиентов.

Список использованных источников

1. Жуков, Н., Информационная безопасность на объекте информатизации банка. Практическое руководство/Н.С. Жуков, А.Ю. Кораблев, Ю.Н. Мельников – Москва: Вестник Ассоциации Российских банков № 27–33. – 1997.

2. Учебное пособие по курсу «Методы и средства защиты информации» [Электронный ресурс] 2014. – Режим доступа: http://www.melnikoff.com/yuriy/posobie.htm – Дата доступа: 14.03.2014

3. Классификация вредоносных программ [Электронный ресурс] 29.10.2013. – Режим доступа: http://blog.kaspersky.ru/klassifikaciya–vredonosnyx–programm/htm – Дата доступа: 14.03.2014

4. Проблемы защиты информации в системах электронной обработки. Пути и методы защиты [Электронный ресурс]. 2014. – Режим доступа: http://lib.nspu.ru/umk/bd311356bf2dc2b0/t5/ch1.html – Дата доступа: 14.03.2014.