Режим доступа: http://www.sovetnik.ru, свободный. – Дата доступа: 12.03.2012.

3. Ястребова, Е.М. PR-менеджеры для библиотеки – управленцы современной формации / Е.М. Ястребова // Библиотековедение. – 2002. – № 4. – С. 30-34.

УДК 681.324

Маркевич А.И.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В УСЛОВИЯХ МАССОВОЙ ИНФОРМАТИЗАЦИИ

БНТУ, г. Минск
Научный руководитель: Зуёнок А.Ю.

Информационная безопасность – это состояние защищенности информационной среды в целом, в частности же – сохранность информационных ресурсов государства и защищенности законных прав личности и общества в информационной сфере. Информационная безопасность (ИБ) играет важную роль в существовании и развитии любого государства, а в условиях массовой информатизации обретает особое значение.

Выделяют следующие составляющие информационной безопасности:

– законодательная, нормативно-правовая и научная база;

– структура и задачи органов (подразделений), обеспечивающих безопасность информационных технологий (ИТ);

– организационно-технические и режимные меры и методы;

– программно-технические способы и средства обеспечения информационной безопасности.

Особое внимание заслуживает четвертая составляющая ИБ. Данная составляющая непосредственно связана с совершенствованием программного обеспечения и аппаратных средств приема, передачи, разрушения и защиты информации.

Суть в том, что техническая сторона ИБ заключается в постоянной гонке технологий и методик, постоянной борьбе злоумышленников и соответствующих государственных органов. Во многом, именно этой гонке обязано прогрессивное развитие электронных и информационных технологий, что также дало скачок развитию информационной безопасности. Таким образом – преступления в области высоких технологий являются важным звеном развития ИБ. В 2011 году были выявлены следующие тенденции:

- использование социальной инженерии;
- развитие технологий сокрытия;
- отклик на мировые события;
- использование уязвимостей;
- появление специализированных угроз.

Наиболее популярной тенденцией является использование социальной инженерии, которая базируется на незнании пользователями основ сетевой безопасности. Для злоумышленника становится гораздо проще хитростью выудить информацию из системы, чем взломать её. В связи с этим в 2011 появилось большое количество вредоносных программ, которые реализуют принципы социальной инженерии:

– **Trojan.Winlock**, блокирующий работу ОС Windows. Семейство Trojan.Winlock существует ещё с 2007 года. Лето 2011 года ознаменовалось появлением «национального» экземпляра Trojan.Winlock, ориентированного на белорусских пользователей Windows и требующего у них передать злоумышленникам некоторую сумму в белорусских рублях на электронный кошелек WebMoney. Главные причины широкого распространения этой угрозы – невнимательность либо некомпетентность пользователей, оказывающихся жертвами вымогателей;

– **Trojan.ArchSMS** (фальшивый самораспаковывающийся архив). Как правило, вредоносная программа загружается пользователем из сети Интернет под видом самораспаковывающегося архива (исполняемого файла), содержащего требуемый пользователю файл. Пользователь, запустив исполняемый файл, наблюдает на мониторе процесс, похожий на распаковку. Но в определенный момент «распаковка» останавливается, и появляется сообщение о том, что для окончания распаковки архива необходимо отправить с мобильного телефона платное SMS-сообщение. При этом размер самого файла близок к «оригиналу» запрашиваемой информации.

С середины 2011 года наблюдалось значительное уменьшение количества фальшивых антивирусов (FakeAV**)**, программ, которые находят на компьютере пользователя множество несуществующих вирусов и для «чистки» предлагают активировать себя через SMS на определенный адрес.

Следующей значимой тенденцией является отклик на мировые события. Последние месяцы 2011 года не стали исключением. Так, после смерти 5 октября основателя компании Apple Стива Джобса мошенники распространяли информацию о бесплатных устройствах iPad «в память о Стиве Джобсе». Пройдя по ссылке, предложенной злоумышленниками, пользователей перенаправляли на вредоносные сайты.

Использование уязвимостей является одной из самых динамичных тенденций. Новым направлением стало активное использование злоумышленниками уязвимостей платформы Java, являющейся самым слабым элементом в защите операционных систем, на которых она установлена. В этом году хакеры, как и в предыдущие годы, активно использовали уязвимости в веб-приложениях, в системах обработки файлов и сервисах сообщений операционной системы.

Ещё одной тенденцией являются специализированные угрозы, целью которых является промышленный и правительственный шпионаж. Например:

– в октябре 2011 появились сообщения о повышенной активности червя Duqu, который имеет сходство с компьютерным червём Stuxnet. Главная задача Duqu – сбор конфиденциальных данных об имеющемся на предприятии оборудовании и системах, используемых для управления производственным циклом. Это может быть любая информация, которая пригодится при организации нападения: снимки с экрана, журналы нажатых клавиш, список запущенных процессов, данные учётных записей, названия открытых окон, сетевая информация, сведения о домене, имена дисков, файлов и пр.

– также в октябре была обнаружена программа «Bundestrojaner», которая по своей природе аналогична вирусу, следит за интернет-браузером, перепиской в Skype, электронной почтой. Немецкие госслужбы использовали эту шпионскую программу «Bundestrojaner» около 100 раз. Программа может делать снимки с экрана, которые в немецких судах рассматриваются в качестве доказательств. Помимо прослушки телефонных разговоров и слежки за перепиской, на зараженном компьютере можно дистанционно включить микрофон или веб-камеру. Данные события представляют собой примеры промышленного и правительственного шпионажа.

Что касается компьютерных преступлений в Беларуси, то 90% из них связаны с банковскими карточками и носят название кардинг. Количество эмитированных банковских карт в Беларуси составляет около 6,5 млн., в то время как пользователей Интернета не более 3,6 млн. Популярность кардинга повышает потребность банковской сферы в информационных технологиях. Со временем же, информационные технологии проникнут в нашу жизнь еще глубже и в других сферах,

что приведет к увеличению ценности информации и к развитию киберпреступности в самых различных отраслях.

Киберпреступники по-прежнему «живут» за счет кражи учетных записей систем онлайн-банкинга, массовой рассылки спама, вымогательства и мошенничества посредством бесчисленных «блокировщиков» и «шифровальщиков» Windows.

ТОП-10 вредоносных программ по статистике антивирусной лаборатории за 2011 год:

1. Trojan-Ransom.FakeAV (трояны-шифровальщики, фальшивые антивирусы);
2. Trojan-PSW.Zbot (трояны, предназначенные для получения паролей и прочей конфиденциальной информации, но не использующие слежение за клавиатурой);
3. Worm.Palevo (Rimecud) (червь, имеющий функционал бэкдора, способен по команде злоумышленника осуществить загрузку файлов на зараженный компьютер. Отправляет на адрес злоумышленника сохраненные пароли из браузеров);
4. Hoax.ArchSMS (Pameseg);
5. Backdoor.TDSS (Alureon, Olmarik);
6. Backdoor.Sinowal;
7. Trojan-PSW.SpyEye;
8. Trojan-Ransom.Cidox;
9. Trojan-Ransom.Winlock;
10. Backdoor.Maxplus (ZAccess).

Динамика роста вредоносных программ остаётся постоянной. Вирусы и трояны усложняются, увеличивается масштаб их распространения, а также скорость, с которой они поражают компьютеры пользователей. В 2011 году, как и прогнозировалось, увеличилось число угроз, работающих на 64-битных платформах. Люди, как и прежде, остаются самым уязвимым звеном в обеспечении информационной безопасности. Однако самое важное, что общая картина информационной безопасности

Беларуси свидетельствует о наличии надежной инфраструктуры, присущей только сильному государству. Что касается органов, обеспечивающих безопасность ИТ, то в Беларуси ключевыми являются:

– оперативно-аналитический центр при Президенте Республики Беларусь,

– управление «К»,

– комитет государственной безопасности.

Данные органы, благодаря своей четкой структуре и профессиональному опыту, обеспечивают максимально надежный уровень информационной безопасности в Республике.

Все составляющие информационной безопасности в Беларуси являют собой четко выстроенную систему с высокой динамикой развития.

УДК 65.78

Новиков В.А.[1], Маркова Е.С. [2]

ИСПОЛЬЗОВАНИЕ ЛОГИСТИЧЕСКОЙ ЦЕПОЧКИ ДЛЯ РЕШЕНИЯ ЗАДАЧИ КОММИВОЯЖЕРА

[1] БНТУ, [2] Высший государственный колледж связи, г. Минск

Задача коммивояжера является ключевой в логистической практике. Эта– задача является базовой для более полных с логистических позиций задач о «рюкзаке» и о Гамильтоновом пути. Предлагаемая методика решения задачи коммивояжера может быть достаточно просто перенесена и на указанные задачи.

С алгоритмической точки зрения задача коммивояжера относится к классу NP-полных задач, поэтому здесь важна простая модель ее решения с учетом неизбежного полного перебора вариантов ответа.

В качестве исходного данного в задаче задается матрица *A* расстояний между городами: