защиты информации, оперативно-технические характеристики которых определяются новыми информационными технологиями. Сегодня стеганография позволяет не только успешно решать основную задачу – скрытно передавать информацию, но и решать целый ряд других актуальнейших задач, в том числе, помехоустойчивой аутентификации, защиты от несанкционированного копирования, мониторинга информации в сетях связи, поиска информации в мультимедийных базах данных и др.

Литература:

1. Грибунин В.Г. и др. Цифровая стеганография. - М.: СОЛОН-Пресс, 2002. - 299 с.
2. Карасев Андрей. Компьютерная тайнопись – графика и звук приобретают подтекст. – //Мир ПК. - № 1/2007. – С.132-134.
3. Специальная техника//№№ 5/1998, 6/1999, 6/2000, 3/2002.
4. Тигулев Максим. Стегонозавр или тайнопись на компьютере. - //Internet журнал http://www.gagin.ru/internet/8/12.html
5. Privacy Guide: Steganography. http://www.all-nettools.com/privacy/stegano.htm
6. http://www.citforum.ru/internet/securities/stegano.shtml
7. http://www.securitylab.ru/analytics/216270.php
8. http://st.ess.ru/publications/articles/steganos/steganos.htm

ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И РОЛЬ ЧЕЛОВЕКА В ИНФОРМАЦИОННОЙ СИСТЕМЕ

Александр Каминский,
эксперт (Республика Молдова)

This work describes the global and local problems of information security, as well as man's role in the common information system.

Централизация знаний и информации происходит на высших уровнях. Идеи и мысли, всё тщательным образом отфильтровывается и обрабатывается, сохраняется и используется для управления низшими звеньями. Тут, применимо высказывание, принадлежащее философу Френсису Бэкону, которое в своё время употребили и приме-

няли на практике Ротшильды: «Кто владеет информацией - владеет миром». Так значит, защищаться, защищать и нападать может лучше тот и те, кто обладает большим количеством качественных знаний и владеет нужной информацией. Нам, если мы хотим создать защищенную систему, нужно карабкаться и рваться вверх по лестнице знаний, находить решения глобального характера, а не зацикливаться только на специфики своей деятельности.

Защиту любой структуры или обычных людей можно сравнить с волнорезами в портах и гаванях. Волнорез обычно строят чуть выше уровня моря, так и организации стараются защитить свою систему чуть выше ныне существующих угроз, чуть «выше уровня моря», но это только создаётся иллюзия безопасности. Многим приходилось, наверно, видеть как во время шторма в море волны свободно перегибают высоту волнореза и в спокойной до того гавани, начинаются колебания и волнения. Если в идеальных условиях волнорез в крупном порту может и не удастся разрушить волной, только разве цунами. То после продолжительного и изощренного шторма на «волнорез» информационной системы, да и на любую другую систему организации, в защите могут появиться сильные пробоины и тогда итог может быть ещё либо известен, либо уже не известен. Примером такого «шторма», в реальности, может быть масштабная атака не только на одну компанию, но и на прилегающие к ней инфраструктуры. Этот процесс может коснуться не только защищающей системы, но и отдельных участников информационной системы. Так можно «оградиться огромнейшими сооружениями» создать идеальную политику безопасности, обучать, наказывать и поощрять членов информационной системы (ИС), но слабейшим звеном остаётся, как бы ни было обидно, сам Человек, инсайдер.

Компьютерные программы и системы, пока они не обладают Искусственным интеллектом, способны действовать только в рамках поставленных на них задач придерживаясь строгих алгоритмов и логики, и только человек может изначально изменить эту логику и соответственно задачи, или в процессе выполнения задачи нарушить логику и алгоритм работы системы.

Построение любой системы начинается с изучения и рассмотрения регламентирующей и законодательной документации, придерживаясь строгих стандартов, если производство большое возможна разработка собственных стандартов. В сфере ИТ, а в частности в ИБ существуют строго регламентированные стандарты такие как: международные стандарты ИБ *ISO/IEC 17799* и ***ISO13335***, а также серия стандартов управления

ИБ ***ISO27000***. Это очень хорошо что «велосипед уже создан», и нам остаётся только использовать и придерживаться этих стандартов и рекомендаций в своей деятельности. Но и злоумышленники придерживаются в своей неблагородной деятельности этих же стандартов. Если все принципы, на которых основывается безопасность ИС, заранее известны, то инструменты как нарушить безопасность системы можно подобрать.

Заботясь о своей национальной безопасности или защищая свою информационную - корпоративную систему, здравым смыслом было бы разрабатывать и использовать собственные принципы защиты, строить безопасность и информационные системы таким образом, чтобы они имели определённую неизвестную специфику. А когда нам «сверху» диктуют как и что, и у кого мы должны покупать, как мы должны защищаться, какие средства защиты на сегодня самые надёжные, какую операционную систему использовать, то о какой специфике и индивидуальности нашей системы может идти речь. Не ужели, более 90% использования операционных систем одной корпорации, и более 50% всех поисковых запросов другой корпорации, в мире в общем - это чистая случайность? О какой глобальной, национальной и тем более корпоративной и личной безопасности может идти речь, когда мы все одинаковые? Мы все сидим на «дырявом» софте, пользуемся прослушивающими сервисами и самое страшное, что мы это всё пускаем в свою корпоративную систему и частную жизнь.

Защита интересов бизнеса и граждан, должна исходить в первую очередь от государства, оно должно на законодательном и исполнительном уровне защищать свои национальные интересы, а не интересы бизнеса других стран. Это если говорить на глобальном и государственном уровне.

А если придерживаться границ частного бизнеса, то защита на этом уровне должна складываться из:

- поиска существующих угроз, реальных для этого сегмента рынка и деятельности организации. Не стоит перегибать палку и приписывать себе угрозы которые могут и не коснуться вас.
- оценки и управления рисками, которые может понести ИС и бизнес в результате действия угроз.
- выбрать оптимальную защиту, и построить ИС таким образом чтобы затраты на защиту были оправданы возможным риском.

Можно сказать, что никогда не будет создана идеальная система защиты, так как знания защищающейся стороны, и тех сторон которые её защищают будут ниже возможных ре-

альных угроз, которые ещё не известны или известны были заранее, но их преднамеренно скрывали. Но попытаться сделать что-то своё всё таки стоит, не стоять на месте, а двигаться вперёд, вверх по лестнице знаний.

Литература и интернет ресурсы:

1. http://ru.wikipedia.org/
2. http://www.intuit.ru/
3. http://www.securitylab.ru/
4. http://security.ase.md/

BPMS – ОСНОВА РЕИНЖИНИРИНГА БИЗНЕС-ПРОЦЕССОВ ПРЕДПРИЯТИЙ

К. Шишманов,
Экономическая академия им. Д.А.. Ценов (Болгария)

Согласно результатам исследований ведущих исследовательских учреждений системы управления бизнес-процессов (Business Process Management System – BPMS или BPM) в настоящий момент являются одним из самых актуальных задач для большинства информационных подразделений предприятий. В связи с этим аналитики IDC ожидают, что к 2011 году продажи систем BPM будут составлять около 5,5 млрд. $ и это примерно 40 % роста в год[1].

BPM системы помогают моделировать процессы, основываясь на анализе потребностей предприятия, для преобразования реальных исполняемых процессов. Уровень развития технологии организации в большой степени определяет и уровень применения BPM. Этот вопрос индивидуального выбора. Некоторые предприятия применяют инструменты моделирования и обмена данными, другие внедряют системы активного контроля рабочих процессов (workflow), третьи обеспечивают трасляцию построенных моделей в новые исполняемые процессы без дополнительного программного кода и т. д. В зависимости от того, какими процессами следует управлять, могут применяться все функции современных BPMS или их часть для решения локальных проблем.

Эмпирический анализ BPM только с точки зрения информационных технологий позволяет сделать следующие выводы:

[1] http://cio.bg/2334_klyuchovi_aspekti_pri_vnedryavaneto_na_bpm