УДК 004.056

Б.Н. Епифанцев

Борьба с инсайдерскими угрозами: системный подход

Приведены модель прироста инсайдерских атак и структура системы, направленной на снижение их числа. Рассмотрены принципы функционирования каждого элемента системы.

В течение многих лет основное направление зашиты информационных ресурсов от несанкционированного доступа строилось на нейтрализации внешних угроз. В последние годы было осознано, что наиболее опасной угрозой ИТ-безопасности являются инсайдеры. Если не учитывать клиентов и партнеров, то за 60% всех инцидентов нарушения безопасности несут ответственность нынешние, бывшие и временные сотрудники компаний. За счет внутренних инцидентов потери мировой экономики в 2006 г. оценивались в 700 млрд долл., средний ущерб от инсайдерской атаки составил 355 тыс. долл. [1]. Приведенные цифры дают основание считать, что нейтрализация внутренних угроз становится определяющей в стратегии борьбы за безопасность информационных ресурсов.

Чтобы определиться с контурами такой стратегии, следует обозначить причины, порождающие инсайдерские атаки. Обобщая известные соображения на этот счет, можно прийти к модели вида

$$\frac{dN_1}{dt} = k_1\frac{D}{P}N_1 - k_2N_1^2 - k_3qN_1 - k_4\alpha N_2 + k_5(D-3)N_1 + k_6(0,03N_3 + 1806) - \\ - k_7(\text{НЗО}(t)/\text{НЗО}(90)) - k_8З_{\text{ПР}} - k_9З_{\text{АК}}.$$

Приращение числа внутренних атак dN_1/dt зависит от отношения среднего дохода от операции к расходу на ее проведение D/P, численности инсайдеров на текущий момент N_1, степени опасности быть пойманным и наказанным q, профессионализма сотрудников службы безопасности α и их числа N_2, различия между средним доходом от операции и зарплатой обслуживающего информационные системы персонала $(D-З)$, числа сотрудников организации, работающих в Internet N_3, отношения нравственного здоровья общества в текущий период к аналогичному показателю 1990 г. $\text{НЗО}(+)/\text{НЗО}(90)$, затрат предприятия на защиту от внутренних угроз $З_{\text{ПР}}$, затрат предприятия на привлечение сотрудников по обслуживанию информационной инфраструктуры в его акционеры $З_{\text{АК}}$.

Степень влияния каждого из перечисленных факторов на приращение dN_1/dt определяется нормирующими коэффициентами $k_1 - k_9$.

За исключением факторов при коэффициентах k_4, k_7, k_9 остальные обсуждались на страницах общедоступных печатных источников. Учет обозначенных факторов под номерами 4, 7, 9 при формировании защиты информационных ресурсов в системах организационного управления поясняется рис. 1.

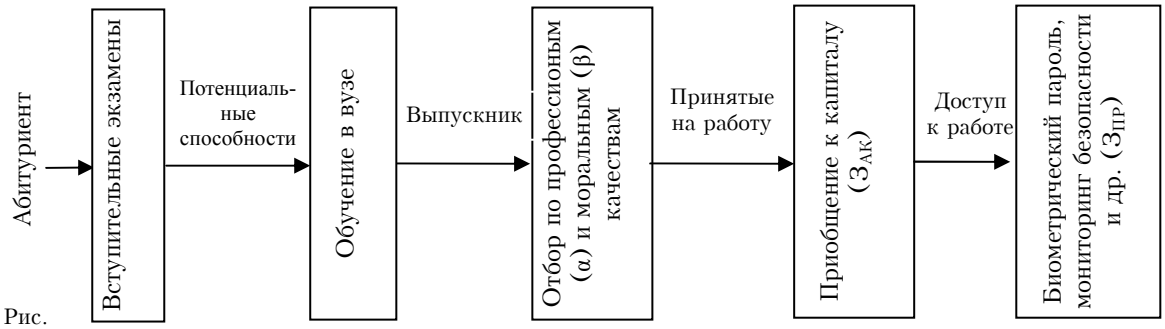

Рис. 1. Подсистема отбора кадров и доступа их к работе при формировании защиты информационных ресурсов в системах организационного управления

Японский принцип «подготовки кадров с пеленок» разумно рассмотреть со стадии поступления в вуз. Организация, ориентированная на решение кадрового вопроса в рамках целевой подготовки, заинтересована в отборе способных студентов. В рамках программы «Выбор профессии» английские ученые создали оригинальную систему тестирования, позволяющую выявлять потенциальные возможности испытуемых для работы в выбранном диапазоне профессий [2]. Приложение методики Дж. Баррета к студентам для оценки природных способностей, необходимых для работы в сфере информационной безопасности, не вызывало оптимизма. Почти 42% подготавливаемых специалистов по направлению «Информационная безопасность» не соответствовало требованиям методики.

Механизм отбора кадров для работы в различных звеньях информационной инфраструктуры не создан. Частные решения этой задачи ориентированы на проверку профессиональных знаний в рамках неформальных бесед. Кривая «профессиональный уровень α – затраты на подготовку специалиста» имеет логический (S-образный) характер. По существующим оценкам $\alpha = 0,2 - 0,6$, и при отсутствии формализованных процедур отбора ошибки неизбежны. В то же время при низкой квалификации персонала ($\alpha < 0,5$) построить эффективную защиту информационных ресурсов невозможно. Эту истину хорошо усвоили зарубежные партнеры. Корпорации Xerox и IBM ежегодно тратят на повышение квалификации более 2000 долл. на сотрудника (~1,5% оборота) [3], чем нивелируются недоработки обучения в университетах.

Другой фактор влияния – «нравственное здоровье общества» характеризует социальные, психические, духовные и эмоциональные составляющие сотрудника. На современном этапе НЗО оценивают по состоянию духовной среды (посещаемость музеев, театров; подписка на периодическую печать и т.д.), состоянием образованности населения и его законопослушностью. Существует технология оценки уровня НЗО. По данной технологии нами проведено исследование динамики НЗО с 1990 г. и связь его с числом зарегистрированных компьютерных преступлений. Эта связь характеризуется коэффициентом корреляции (– 0,7) – слишком большой величиной, чтобы не обратить на нее внимание ответственным за НЗО религиозным и государственным организациям страны.

В свою очередь нравственное здоровье сотрудника определяется его морально-психологическими показателями (индекс β на рис.1). С помощью экспертных технологий выделено 9 таких показателей, оценен их вес и найдены способы их количественной оценки у испытуемых с использованием полиграфа. Отрабатывается технология отбора на базе «Эгоскопа». Конечный результат отбора – вероятность сотрудника нарушить принятые обязательства в тех или иных условиях.

Проблема инсайдерства в информационном обществе изучалась известным ученым М. Кастельсом. По его мнению, лица, обеспечивающие функционирование информационной инфраструктуры организации, фактически получили право управления организацией в целом. Их недовольство развитием событий или неучет их мнения при принятии решений могут выражаться в действиях, направленных на разрушение организационной системы специфическими методами, противостоять которым невозможно [4]. Лучший выход – привлечь их в число акционеров. Эта позиция отражена на рис. 1 введением блока «Приобщение к капиталу».

В последние годы для борьбы с инсайдерскими угрозами используют мониторинг Интернет-трафика, системы мониторинга рабочих станций и электронной почты, организационные меры, комплексные решения. Эти меры дают временный эффект в соревновании со злоумышленниками. Поэтому наблюдается всплеск интереса к биометрическим технологиям, особенно тем из них, которые основаны на анализе поведенческих неосознаваемых движений.

По изложенным материалам можно сделать однозначный вывод. Сдвиг интереса научного сообщества к борьбе с внутренними угрозами информационной безопасности очевиден. Сформировались контуры стратегии в борьбе «брони и снаряда». Осознана необходимость наличия разнородных инструментов регулирования внутренних угроз. Однако сохраняется неясность эффективности предложенных инструментов и, следовательно, оптимальной схемы борьбы с инсайдерством.

Литература

1. Скиба В.Ю., Курбатов В.А. Руководство по защите от внутренних угроз информационной безопасности. – СПб.: Питер, 2008. – 320 с.

2. Баррет Дж. Карьера: способности и выбор. – М.: ООО «Изд-во АСТ», 2003. – 2004 с.

3. Стратегия эффективности формирования и использования знаний // Business. – 2003. – № 6. – С. 40–41.

4. Кастельс М. Информационная эпоха: экономика, общество и культура. – М., 2000. – 608 с.

Епифанцев Борис Николаевич
Сибирская государственная автомобильно-дорожная академия
Профессор факультета информационных систем в управлении
Эл. почта: epifancev_bn@sibadi.org

B.N. Epifancev

Struggle with insiders attacks: the system approach

The model of a gain insiders attacks and structure of the system directed on decrease of their number is resulted. Functioning principles of each systems element are considered