ОЦЕНКА ЗАЩИЩЁННОСТИ ПОЛЬЗОВАТЕЛЯ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОТ СОЦИОИНЖЕНЕРНЫХ АТАК НА ОСНОВЕ КОМПЛЕКСА "КРИТИЧНЫЕ ДОКУМЕНТЫ–ИНФОРМАЦИОННАЯ СИСТЕМА–ПЕРСОНАЛ–ЗЛОУМЫШЛЕННИК"[1]

Абрамов М.В., м.н.с. лаб. теоретических и междисциплинарных проблем информатики Санкт-Петербургского института информатики и автоматизации Российской академии наук, ст. преп. кафедры информатики СПбГУ, mva16@list.ru

Аннотация

В докладе рассмотрены усовершенствованные модели комплекса «критичные документы–информационная система–персонал–злоумышленник». На основе этих моделей получена новая оценка вероятности успеха социоинженерной атаки злоумышленника на пользователя. На данной оценке основывается вывод о защищённости пользователей информационной системы от подобных атак. Новая оценка агрегирует более широкий круг параметров, чем предыдущая.

Введение

Широкое распространение информационных технологий сегодня заставляет уделять большое внимание вопросам информационной безопасности (ИБ). В последнее время атаки на информационные системы стали происходить чаще, приносить большие убытки и требовать больше ресурсов и времени для установления виновных в подобных преступлениях [13].

В настоящее время большая часть исследований в области обеспечения ИБ посвящена программно-техническим аспектам [1–4,9–11]. В таком срезе вопросы ИБ достаточно хорошо изучены, разработано большое количество средств, позволяющих снизить вероятность успеха программно-технической атаки злоумышленника. В то же время

[1] Работы выполнялись в рамках проекта по государственному заданию СПИИРАН № 0073-2014-0002.

пользователь информационной системы, к данным которой злоумышленник пытается получить доступ, является одним из ее самых уязвимых мест [12]. Согласно [8], наиболее распространённые инциденты ИБ так или иначе связаны с действиями пользователей системы. Одним из наиболее эффективных видов атак на ИБ является корпоративный шпионаж, которому подвергаются более четверти компаний и почти 80% из них успешно [8].

Таким образом, проблемы ИБ и защиты пользователей от социоинженерных атак, т.е. атак, направленных в первую очередь на персонал, в настоящее время весьма актуальны. Исследования в этой области помогут в создании многоуровневых систем безопасности, более устойчивых к атакам злоумышленников.

Общая цель направления исследований заключается в построении оценки защищённости персонала информационных систем от социоинженерных атак. Под защищённостью персонала понимается степень его устойчивости к социоинженерным атакующим воздействиям злоумышленника (САВЗ). Цель настоящей работы — предложить подход к оценке вероятности успеха САВЗ на пользователя информационной системы. Указанная цель достигается за счет агрегирования сведений о более широком круге факторов, влияющих на оценку вероятности успеха САВЗ. Оценка позволит выявлять наиболее уязвимые звенья системы и своевременно предпринимать необходимые меры по обеспечению защиты информации.

Возросшая сложность компьютерных сетей и механизмов защиты [10], увеличение количества уязвимостей пользователей, а также возможностей по реализации атак обуславливает необходимость разработки мощных автоматизированных средств (систем) анализа защищенности. Эти системы призваны выполнять задачи по обнаружению уязвимостей пользователей информационной системы, информированию служб безопасности, выявлению возможных трасс атакующих действий нарушителей, определению критичных сетевых ресурсов и выбору адекватной угрозам политики безопасности, которая задействует наиболее подходящие в заданных условиях защитные механизмы. Уязвимость пользователя определяется по аналогии с программно-технической уязвимостью и заключает в себе некоторую характеристику пользователя, которая делает возможным успех САВЗ [7].

Решение этих задач позволит существенно повысить защищенность пользователей информационных систем, то есть уменьшить вероятность успеха атаки злоумышленника на информационную систему. Для увеличения точности данной оценки предлагается расширение модели комплекса «информационная система — персонал — критичные

документы» (ИСПКД) за счет включения профиля компетенций злоумышленника и перехода к более полной модели, а именно «критичные документы — информационная система — персонал — злоумышленник» (КДИСПЗ). В статье наиболее подробно рассмотрен подход к моделированию злоумышленника в рамках данной парадигмы и идея формирования профиля компетенций, включённого в модель.

Оценка вероятности успеха

В работе [5] была предложена модель комплекса КДИСПЗ дополняющая комплекс ИСПКД [6] моделью злоумышленника. Комплекс представлен на рисунке 1. В основе модели злоумышленника лежит профиль компетенций злоумышленника (ПКЗ). Профиль компетенции злоумышленника может быть представлен в следующем виде: $((R_1, D(R_1)),...,(R_k, D(R_k)))$, где R_i — это ресурс, доступный злоумышленнику, а $D(R_i)$ — количество или объем ресурса, доступного злоумышленнику. Вероятность успеха социоинженерного атакующего воздействия j-ого злоумышленника с использованием i-ого ресурса на k-ого пользователя рассчитывается по формуле

$$p_{ij} = \frac{D_j(R_i) S_k(V_l, R_i)}{M_i B_l},$$

где $D_j(R_i)$ — выраженность ресурса R_i у злоумышленника j, $S_k(V_l, R_i)$ — выраженность уязвимости V_l, на которую можно воздействовать с помощью ресурса R_i, у пользователя k, M_i — максимальная выраженность ресурса R_i, B_l — максимальная выраженность уязвимости V_l. График распределения для данной вероятности успеха социоинженерной атаки показан на рисунке 2.

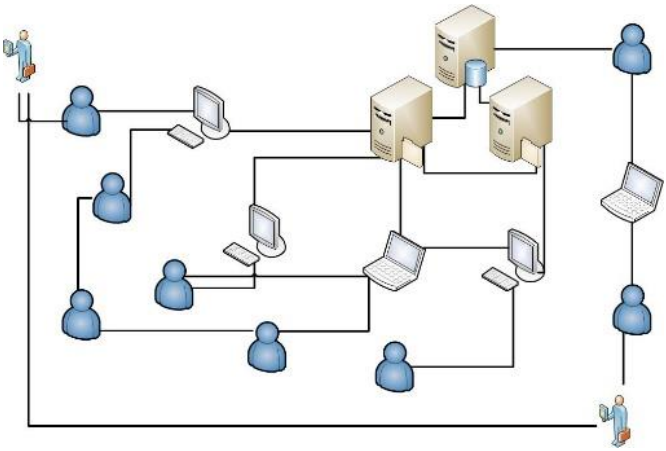

Рис. 1. Комплекс «критические документы – информационная система – персонал – злоумышленник».

Заметим, что в ряде случаев при моделировании САВЗ могут быть получены некорректные оценки вероятности успеха этих воздействий. Так, например, в случае, если модели пользователя сопоставлен профиль уязвимостей пользователя (ПУП), содержащий высокие оценки выраженности уязвимостей пользователя, и, при этом, модели злоумышленника сопоставлен ПКЗ, содержащий низкие оценки его компетентности, то расчетная вероятность успеха имитированной социоинженерной атаки будет невысока. В то время как это противоречит основной идее ПУП, которая говорит о том, что при высокой степени выраженности уязвимостей пользователя, данный пользователь наиболее подвержен САВЗ вне зависимости от его умений и навыков. Справедливо и обратное, если модели злоумышленника сопоставлен ПКЗ, содержащий высокие оценки его компетентности, а модели пользователя сопоставлен ПУП, содержащий низкие оценки его уязвимостей, то вероятность успешности социоинженерного атакующего воздействия будет также мала. При этом очевидно, что влияние степени выраженности уязвимостей, содержащихся в ПУП, и степени проявления компетенций злоумышленника, содержащихся в ПКЗ, на расчетное значение

вероятности имитируемого САВЗ различно. Изменим формулу следующим образом для получения более точных результатов:

$$p_{ij} = \frac{\left(\frac{S_k(V_l, R_i)}{B_l} - \alpha\right)^2 \left(\frac{D_j(R_i)}{M_i} - \beta\right)^2}{(1-\alpha)^2 (1-\beta)^2}.$$

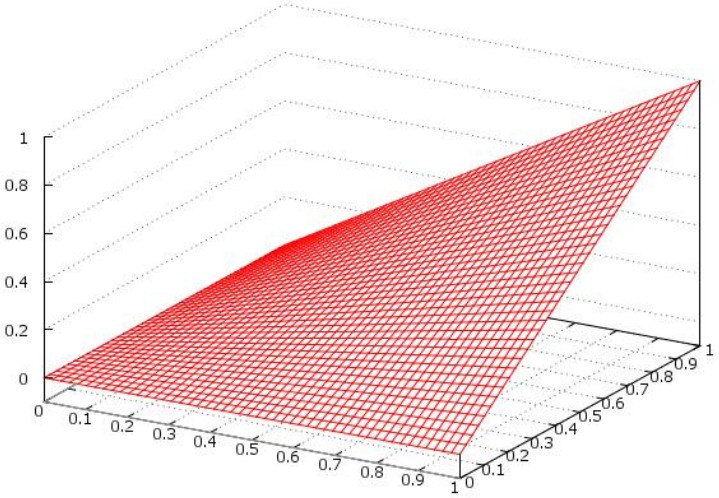

Рис. 2. График распределения вероятности успеха социоинженерной атаки, построенный для первой формулы.

В зависимости от параметров α и β осуществляется сдвиг, позволяющий усилить влияние выраженности уязвимости пользователя или уровня компетенции злоумышленника на итоговое значение вероятности. Параметры α и β являются показателями влияния факторов, содержащихся в ПУП и ПКЗ, на расчетную вероятности успеха САВЗ на пользователя информационной системы. На рисунке 3 представлен график распределения вероятностей успеха имитируемого САВЗ на пользователя информационной системы, построенный для значений $\alpha = 0.30$, $\beta = 0.15$. Данные значения показывают, что влияние степени проявления уязвимостей пользователя, содержащихся в ПУП, выше, чем степень выраженности компетенций злоумышленника, содержащихся в ПКЗ.

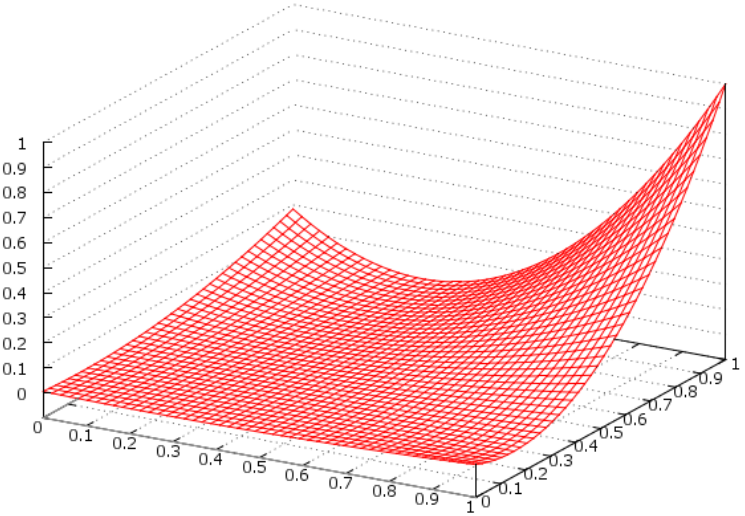

Рис. 3. График распределения вероятности успеха социоинженерной атаки, построенный для значения $\alpha = 0.30$, $\beta = 0.15$.

Заключение

В статье приведён подход к оценке успешности САВЗ на пользователя информационной системы. Получены более точные приближения, основанные на агрегировании сведений о более широком круге факторов, влияющих на оценку вероятности успеха САВЗ.

Литература

1. *Distefanoa S., Puliafitob A.* Information dependability in distributed systems: The dependable distributed storage system // Integrated Computer-Aided Engineering 21 (2014). P. 3–18.
2. *Goo J., Yim M. S., Kim D. J. A* Path to Successful Management of Employee Security Compliance: An Empirical Study of Information Security Climate //Professional Communication, IEEE Transactions on. Т. 57. №. 4. 2014. С. 286-308.
3. *James C.* Information systems user security: A structured model of the knowing–doing gap // Computers in Human Behavior. Sep2012. Vol. 28. Issue 5. P. 1849–1858.
4. *Trčcek D., Trobec R., Pavešsić N., Tasič J.F.* Information systems security and human behaviour. // Behaviour & Information Technology. Mar-Apr 2007. Vol. 26. Issue 2. P. 113–118.
5. *Абрамов М.В., Азаров А.А., Тулупьева Т.В., Тулупьев А.Л.* Модель профиля компетенций злоумышленника в задаче анализа защищённости персонала информационных систем от социоинженерных атак //Информационно-управляющие системы. 2016. №4. С. 77–84
6. *Азаров А. А.* Вероятностно-реляционные модели и алгоритмы обработки профиля уязвимостей пользователей при анализе защищённости персонала информационных

систем от социоинженерных атак // Диссертация на соискание учёной степени к.т.н. 2013
7. *Бычек В., Ершова Е.* Социальная инженерия в интеллектуальной битве «добра» и «зла» // Защита информации. Инсайд, №6 2006.
8. Информационная безопасность бизнеса. Исследования текущих тенденций в области информационной безопасности бизнеса // Лаборатория Касперского. URL: http://media.kaspersky.com/pdf/IT_risk_report_Russia_2014.pdf (дата обращения: 30.04.2015)
9. *Котенко И.В., Степашкин М. В.* Системы-имитаторы: назначение, функции, архитектура и подход к реализации // Изв. вузов. Приборостроение. 2006. Т. 49, № 3. С. 3–8.
10. *Котенко И.В., Степашкин М.В.* Анализ защищённости компьютерных сетей на основе моделирования действий злоумышленников и построения графа атак // Труды ИСА РАН. 2007. Т. 31. С. 126–207.
11. *Котенко И.В., Юсупов Р. М.* Перспективные направления исследований в области компьютерной безопасности. Защита информации. Инсайд. 2006. № 2. С. 46.
12. *Сапронов К.* Человеческий фактор и его роль в обеспечении информационной безопасности. URL: http://www.interface.ru/home.asp?artId=17137 (дата обращения 05.03.2015).
13. Убытки от киберпреступлений продолжают расти // URL: http://www8.hp.com/ru/ru/software-solutions/ponemon-cyber-security-report/index.html (дата обращения 04.03.2015)