АНАЛИЗ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ МОДЕЛЕЙ

А.В. Корвель
Научный руководитель – В.Ф. Алексеев
канд.техн.наук, доцент
Белорусский государственный университет информатики и радиоэлектроники

Одной из задач, с которой сталкивается любая организация, является проблема защиты деловой и частной информации, а также имущества и других объектов от действий злоумышленников. Бурное развитие информационных коммуникаций, расширение масштаба деловой активности и взаимодействия людей облегчает действия злоумышленников. Повышение ценности информации в современном мире делает задачу защиты еще более актуальной.

Защита информации и имущества осуществляется с использованием систем безопасности (СБ), которая имеет аппаратные и программные средства для осуществления задачи безопасности объектов защиты.

Возникновение проблемы информационной безопасности во многом обусловлено широким распространением корпоративных информационно-вычислительных систем со слабо защищенным программно-техническим обеспечением. В этих условиях решение вопросов безопасности в информационной системе (ИС) реализуется с применением различных подходов, в том числе: автоматизированных инструментальных средств оценки рисков несанкционированного доступа (НСД) к информации (CRAMM, RiskWatch, COBRA и др.), автоматизированных средств тестирования, на наличие уязвимостей в информационной системе (ISS, SATAN, COPS и др.), автоматизированных средств проектирования систем.

Данной проблеме посвящено значительное количество работ отечественных и зарубежных исследователей, среди которых В.А. Герасименко, В.В. Мельников, С.С. Корт, А.Г. Корченко, И.В. Котенко, М.В. Степашкин, В.И. Богданов, А.А. Малюк, Д.П. Зегжда, A. Moore, R. Ellison, R. Linger, S. Templeton, K Levitt, Xinming Ou, R.P. Lippman, O. Sheyner, J. Haines, S. Jha, J.Wing, S. Noel, S. Jajodia, M. Bishop, P. Ammann, B. Schneier и другие [1–3].

Существует множество современных международных и отечественных стандартов, нормативных документов в области информационной безопасности, рассматривающих вопросы оценки эффективности СЗИ или определяющих требования к её функциональности.

В этих документах, как правило, в качестве критерия эффективности используется наличие тех или иных средств защиты информации или требования к их параметрам и не учитывается, что имеются возможности

преодоления данных средств за счет наличия в них тех или иных уязвимостей.

Несмотря на значительное количество исследований в этом направлении, отсутствует детальная информация о методах и алгоритмах выбора оптимального проекта СЗИ по критерию эффективности, учитывающему наличие уязвимостей и взаимосвязей между ними.

Автором выполнен анализ типовой структуры информационной системы и её системы защиты. На основании проведенного анализа было показано, что по структуре и принципам функционирования информационные системы типовых коммерческих и государственных организаций подобны корпоративным сетям и могут быть описаны соответствующими моделями.

Показано, что в процессе функционирования системы безопасности состав субъектов и объектов, права субъектов и связи объектов между собой могут динамически изменяться. При рассмотрении вопросов защиты исследования основывались на аксиоме, которая положена в основу американского стандарта по защите («Оранжевая книга») и предполагает, что все вопросы безопасности объектов определяются доступами субъектов к объектам.

Эта аксиома охватывает практически все известные способы нарушения безопасности в самых различных вариантах понимания безопасности. Следовательно, для рассмотрения вопросов безопасности и защиты объектов достаточно рассматривать множество объектов и доступ к ним субъектов.

Показано, что угрозы нарушения конфиденциальности (секретности) направлены на получении доступа к объектам (информации, имуществу) лицам, которые не должны иметь к ней доступ. Это происходит при несанкционированном доступе к некоторым закрытым объектам, который не связан с непосредственным их изменением или повреждением.

Установлено, что для надежной защиты организации от угроз необходимо ограничивать как физический, так и удаленный доступ к объектам защищаемой организации. Для защиты самой системы безопасности в сетевой среде необходимо защищать ее аппаратные средства, данные и линии передачи информации. Это подтверждает представленную аксиому о решающей роли контроля над доступом субъектов к объектам в вопросах обеспечения безопасности.

Для решения поставленных задач использовались: методы теории вероятности и случайных процессов, методы дискретной математики, формальной логики, теория графов, математическое моделирование, теории, технологии и стандарты проектирования и функционирования, информационных систем и вычислительных сетей, теория и методы анализа эффективности и проектирования систем защиты информации.

Для оценки уровня защищенности, реализуемой средствами защиты, применялись формальные и неформальные методы обработки экспертных оценок, для выбора оптимального комплекса средств защиты» использовались методы оптимального проектирования и многоальтернативной оптимизации.

Библиографический список

1. Korchenko A., Prystavka P, Kazmirchuk S., Akhmetov B. Analytical verification expressions of linguistic variables for information security risk assessment systems // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 1, p. 50-55.

2. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения К.: МК-ПресС, 2006. — 320 с.

3. Зегжда Д. П. Основы безопасности информационных систем : Учебное пособие для вузов по специальности "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем " / Д. П. Зегжда, А. М. Ивашко . – М. : Горячая Линия-Телеком, 2000 . – 452 с.