обязанностей по обеспечению ее конфиденциальности путем регламентирования деятельности персонала как по защите информации, так и по обслуживанию информационных систем, а также назначения ответственных за поддержание информационной безопасности на требуемом уровне.

Комплексное применение организационных мер вместе с использованием технических средств защиты, таких как системы авторизации и разграничения доступа, сбора и аудита событий, средств антивирусной защиты и межсетевого экранирования, позволяет перекрыть уязвимые места, усилить действие друг друга и обеспечить надлежащее выполнение задач, поставленных в рамках обеспечения информационной безопасности систем обработки статистических данных.

О НЕКОТОРЫХ МЕТОДАХ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ДЛЯ КРЕДИТНО-ФИНАНСОВЫХ УЧРЕЖДЕНИЙ

Е.В. ВАЛАХАНОВИЧ, Л.В. МИХАЙЛОВСКАЯ

Одна из наиболее актуальных проблем, возникших на современном этапе — это проблема безопасности информации (БИ) в автоматизированных системах обработки информации (АСОИ) вследствие того, что неправомерное искажение, уничтожение или разглашение определенной части информации, дезорганизация процессов ее обработки и передачи наносят серьезный материальный и моральный урон многим субъектам, участвующим в процессах информационного взаимодействия.

Мероприятия по обеспечению БИ являются технически сложными, требуют высокой квалификации исполнителей, специальных знаний, глубокого понимания процессов работы как приложений, обрабатывающих персональные данные, так и средств защиты информации. Вследствие того, что функционирование кредитно-финансовых учреждений (КФУ) невозможно без использования АСОИ, одним из самых важных вопросов в организации БИ является оценка рисков информационной безопасности, от грамотного проведения которого зависит как степень управляемости данными рисками, так и величина расходов на организацию БИ [1].

В работе проведен анализ рисков информационной безопасности: доступности, целостности и конфиденциальности. Разработана шкала ценностей данных рисков и определены уровни важности информационных объектов КФУ.

Проанализированы методы оценки риска: в денежном выражении, вероятностный и балльный, которые позволяют определить соответствующий уровень уязвимости для каждой комбинации информационного актива и угрозы КФУ, а также степень потенциальной опасности угроз [2]. Разработанные методы оценки рисков информационной безопасности на базе теории игр и спроектированные алгоритмы максиминной стратегии и симплекс метода позволяют определить оптимальный комплекс мероприятий по защите информации для КФУ.

Литература

1. *Маслов О.Н.* О моделировании риска принятия решений в области обеспечения информационной безопасности // INSIDE. Защита информации. 2011. № 4.

2. *Валаханович Е.В.* Угрозы информационной безопасности объекта и их классификация // Сборник научных статей Военной академии Республики Беларусь. 2012. № 22.