УДК 004.041

ФОРМИРОВАНИЕ БАЗЫ ДАННЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ ЭКСПЕРТНЫХ ОЦЕНОК

А. С. Романов, Д. А. Жолобов
Астраханский государственный университет (Россия)

В статье рассматриваются вопросы подбора комплекса средств защиты информации, основанные на оценке группы экспертов. Определены критерии средств защиты информации и функции для экспертной оценки. Предлагается построить базу данных с целью последующего оптимального выбора средств защиты информации.

Ключевые слова: *средства защиты информации, критерии оценки, функционал средств защиты информации, база данных, экспертные оценки.*

This article discusses the selection of means of information security based on an evaluation of the expert group. We defined the criteria of information security tools and features for expert evaluation. It is proposed to build a database for subsequent optimal choice of information security solutions.

Key words: *information security means, evaluation criteria, the functional information security tools, database, expert judgment.*

Высочайшая степень автоматизации, к которой стремится современное общество ставит его в зависимость от уровня безопасности используемых информационных технологий. Массовое применение компьютерных

систем, позволившее решить задачу автоматизации процессов обработки изо дня в день нарастающих объемов информации, сделало эти процессы в высшей степени уязвимыми по отношению к агрессивным воздействиям и поставило перед потребителями информационных технологий новую проблему, — проблему информационной безопасности. Минимизировать риски информационной безопасности можно в том числе с помощью средств защиты информации, поэтому проблема подбора средств защиты часто становится одной из основных для ответственного сотрудника организации.

В соответствии с законодательством Российской Федерации в информационных системах ряда организаций использование сертифицированных программных продуктов является обязательным. Данное требование определяется целым рядом положений законодательных и нормативных актов в области защиты информации, в частности приказом № 17 ФСТЭК России от 11.02.2013 г. «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», Федеральным законом Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных», приказом ФСТЭК России от 18.02.2013 г. № 21, законом РФ №5485-I от 21.07.1993 г. и др.

В связи с постоянно растущим количеством сертифицированных средств защиты информации, представленных на рынке, их выбор представляет собой достаточно сложную задачу. Помимо известных на рынке игроков – таких как Cisco Systems Inc., Инфотекс, «Доктор Веб» и другие, представлены и менее крупные, такие как «Элвис-Плюс», CheckPoint Software Technologies Ltd, SafeNet Inc. В настоящее время в реестре сертифицированных средств защиты ФСТЭК представлены около 3000 наименований. Выбор наиболее подходящего комплекса средств защиты для конкретной организации является актуальной и сложной задачей.

Вопрос выбора средств защиты рассматривался в работах [1, 2] и др. Однако, в данных исследованиях не учтены последние изменения в законодательстве, а также отсутствует способ формирования комплексной системы защиты на основе взаимодополняющих продуктов.

В данной работе предлагается подход к формированию комплекса средств защиты информации, основанный на базе данных, представленных на рынке сертифицированных средств защиты. Пользователь, которому необходимо подобрать средства защиты информации, указывает критерии и параметры системы защиты, после чего ему предлагается ранжированный в соответствии с его требованиями список возможных комплектов.

Каждое средство защиты в базе данных проходит экспертную оценку по ряду критериев (табл. 1). Экспертной группой были выбраны 9 критериев и обозначены веса данных критериев. Сумма весов критериев равна 1. Выбор данных критериев обусловлен наличием доступной информации

только о технических возможностях средств, в то время как информация о реальной работе средств в системах защиты отсутствует, либо разрознена.

Таблица 1

Критерии проведения экспертной оценки

Наименование критерия	*Вес*
Отказоустойчивость	0,15
Масштабируемость	0,08
Интеграция с различными платформами	0,13
Квалификация обслуживающего персонала	0,09
Удобство использования	0,11
Техническая поддержка	0,1
Частота, качество обновлений	0,11
Незаметность для пользователя	0,08
Стоимость	0,15

Большинство представленных средств защиты могут выполнять несколько функций по обеспечению информационной безопасности, в связи с этим подбор средств необходимо выполнять таким образом, чтобы обеспечить минимальное «перекрытие» функционала. На основании приказа ФСТЭК № 21 на рассмотрение экспертам был выдвинут следующий функционал, выполняемый средствами защиты информации:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации;
- регистрация событий безопасности;
- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности;
- обеспечение целостности информационной системы;
- обеспечение доступности;
- защита среды виртуализации;
- защита технических средств;
- защита информационной системы, ее средств, систем связи и передачи данных.

Для формирования базы данных средств защиты был разработан и подготовлен паспорт средств защиты информации следующего вида (рис. 1).

Критерии / Функции	Отказоустойчивость	Масштабируемость	Интеграция с различными платформами	Квалификация обслуживающего персонала	Удобство использования	Техподдержка	Частота, качество обновлений	Незаметность для пользователя	Стоимость
Идентификация и аутентификация субъектов доступа и объектов доступа									
Управление доступом субъектов доступа к объектам доступа									
Ограничение программной среды									
Защита машинных носителей информации									
Регистрация событий безопасности									
Антивирусная защита									
Обнаружение (предотвращение) вторжений									
Контроль (анализ) защищенности									
Обеспечение целостности информационной системы									
Обеспечение доступности									
Защита среды виртуализации									
Защита технических средств									
Защита информационной системы, ее средств, систем связи и передачи данных									

Рис. 1. Бланк паспорта средств защиты информации

Межсетевой экран Check Point UTM-1 Edge N										
Критерии / Функции	Отказоустойчивость	Масштабируемость	Интеграция с различными платформами	Квалификация обслуживающего персонала	Удобство использования	Техподдержка	Частота, качество обновлений	Незаметность для пользователя	Стоимость	Итоговая оценка
Идентификация и аутентификация субъектов доступа и объектов доступа	7	3	6	6	6	8	6	7	6	0,687778
Управление доступом субъектов доступа к объектам доступа	7	3	6	6	6	8	6	7	6	0,687778
Ограничение программной среды	0	0	0	0	0	0	0	0	0	0
Защита машинных носителей информации	0	0	0	0	0	0	0	0	0	0
Регистрация событий безопасности	7	3	6	6	6	8	6	7	6	0,687778
Антивирусная защита	0	0	0	0	0	0	0	0	0	0
Обнаружение (предотвращение) вторжений	0	0	0	0	0	0	0	0	0	0
Контроль (анализ) защищенности	0	0	0	0	0	0	0	0	0	0
Обеспечение целостности информационной системы	0	0	0	0	0	0	0	0	0	0
Обеспечение доступности	7	3	7	6	6	7	6	7	6	0,691111
Защита среды виртуализации	0	0	0	0	0	0	0	0	0	0
Защита технических средств	0	0	0	0	0	0	0	0	0	0
Защита информационной системы, ее средств, систем связи и передачи данных	7	3	7	6	6	7	6	7	6	0,691111
Вес критерия	0,15	0,08	0,13	0,09	0,11	0,1	0,11	0,08	0,15	

Рис. 2. Заполненный паспорт средств защиты информации

Экспертная группа проставила оценки каждому средству защиты в диапазоне от 0 до 10. В случае, если данное средство не выполняло какие-либо функции, экспертом проставлялись значения 0 по данной функции.

После получения анкет экспертов происходил итоговый подсчет проставленных экспертами оценок для каждого средства. Подсчет производился по формуле:

$$Z_f = \sum x_{ij} * d_i,$$

где Z_f – итоговое значение для выполняемой функции; x_{ij} – значение функции, относительно критерия; d_i – вес критерия.

Причем если $x_{1j} \leq Z_f$ для критерия «отказоустойчивость», то $Z_f = x_{1j}$, т. к. отказоустойчивость – выход из строя средства защиты – выводит из строя всю систему защиты полностью, т. е. действует эффект «слабого звена».

В итоге для каждого проанализированного средства защиты информации был сформирован паспорт следующего вида (на примере Check Point UTM-1 Edge N), представленный на рис. 2.

Проведенный анализ выбранных критериев и оценки функциональности на основании данных критериев экспертными группами позволит сформировать базу данных средств защиты. Использование подобной базы данных сможет помочь сотруднику организации более эффективно осуществить выбор средств защиты информации для построения системы защиты, опираясь не только на технические данные производителя, но и на мнение экспертов, которые непосредственно работали с различными средствами и смогли произвести субъективную оценку.

Список литературы

1. Нурдинов Р. А. Обоснование целесообразности выбора средств защиты информации // Современные наукоемкие технологии. – 2014. – № 5 (ч. 1). – С. 81–82.

2. Хализев В. Н. Методика выбора оптимального набора средств программно-аппаратной защиты информации // Международная заочная научно-практическая конференция «Физико-математические науки и информационные технологии: теория и практика» (Россия, г. Новосибирск, 26 ноября 2012 г.). – Новосибирск, 2012.