ОПРЕДЕЛЕНИЕ СОСТАВА СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Жарков Г.В.[1], Бабенко А.А.[1]

[1)] Волгоградский государственный университет, г. Волгоград, Россия
E-mail: g89954113431@gmail.com

DETERMINATION OF THE COMPOSITION OF THE INFORMATION PROTECTION SYSTEM IN STATE INFORMATION SYSTEMS

Zharkov G.V.[1], Babenko A.A.[1]

[1)] Volgograd State University, Volgograd, Russia

This article discusses the process of choosing the composition of information protection means in state information systems. A software tool was developed to automate the process of selecting the composition of protective equipment. Each stage of this process is described.

Выбор наиболее эффективного состава системы защиты информации в государственных информационных системах состоит из пяти этапов, причем на каждом этапе необходимы соответствующие данные [1]. Опишем каждый из этих этапов.

Первым этапом является формирование модели угроз и оценка рисков. Для качественной оценки необходимо сведения о составе государственной информационной системы, актуальные угрозы, а также вероятность их возникновения [2]. Результатом анализа является список угроз и рисков, которым подвержена анализируемая государственная информационная система [3].

Второй этап включает в себя создание матрицы отношений между угрозами, определенными на первом этапе, и средствами защиты информации, перекрывающие данные угрозы. Для создания матрицы отношений необходим актуальный список средств защиты.

На третьем этапе происходит экспертная оценка средств защиты информации по таким параметрам, как: срок действия сертификатов ФСТЭК/ФСБ; многофункциональность; соответствие заявленного в программном обеспечении СЗИ уровню контроля на отсутствие не декларированных возможностей; стоимость СЗИ ГИС; количество нейтрализуемых угроз каждым техническим СЗИ в ГИС; величина предотвращенного техническим СЗИ в ГИС риска от реализации угрозы. Помимо применения экспертного метода на данном этапе необходимо знание приемлемого и критического значений рисков на основе присвоенного уровня защищенности, анализируемой государственной информационной системы.

На четвертом этапе осуществляется определение обобщенного показателя эффективности каждого средства защиты информации в государственной информационной системе. Для определения показателя необходимо знание частных

критериев эффективности каждого средства защиты информации, а также знание «эталонного» показателя эффективности.

На последнем этапе происходит непосредственное определение средств защиты с лучшими показателями эффективности [4].

В результате работы данного алгоритма, помимо, определения наиболее эффективного состава средств защиты информации в государственной информационной системе, так получается получить показатели эффективности для каждого средства защиты.

Данный алгоритм реализован в программном комплексе «Определение состава системы технической защиты информации в государственных системах» (свидетельство о государственной регистрации программы №2020615502 от 25 мая 2020 г) [5].

1. Федеральный закон "Об информации, информационных технологиях и о защите информации" от 27.07.2006 N 149-ФЗ
2. В. В. Селифанов, А. С. Гордеев, Д. Г. Макарова, А. А. Старикова, Интерэкспо Гео-Сибирь, 228-232 (2018).
3. Приказ ФСТЭК России от 11 февраля 2013 г. N 17 Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.
4. Методический документ. Меры защиты информации в государственных информационных системах. Утвержден ФСТЭК России 11 февраля 2014 г.
5. Бабенко А.А. Жарков Г.В. Программа определение состава системы технической защиты информации в государственных системах: св-во о гос. рег. прогр. для ЭВМ 2020615502 Российская Федерация. Зарегист. 25.05.2020.