СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ОЦЕНКИ УПРАВЛЕНИЯ РИСКАМИ ПРИ КОНСТРУИРОВАНИИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ В ЗАЩИЩЕННОМ ИСПОЛНЕНИИ

О. Ю. Кондратьева[1], Д. В. Терин[1,2], Е. В. Кондратьева[1]

[1]Саратовский национальный исследовательский государственный университет им. Н. Г. Чернышевского, Россия
[2]Саратовский государственный технический университет им. Ю. А. Гагарина, Россия
E-mail: elka@sgu.ru, terinden@mail.ru

Рассмотрены пути усовершенствования оценивания рисков возникающих в результате эксплуатации элементов автоматизированных систем. Авторы предполагают, что система по определению является защищенной, но ее «несущественные» по функционалу элементы могут стать каналами несанкционированного доступа, количество которых соответствует ожидаемой модели поведения потенциального нарушителя. Рассматриваемая модель оценки рисков показала свою эффективность в системах сегментирования, анализа и маркетирования наукоемкой информации и эмуляции процессов оценки безопасности автоматизированных систем в защищенном исполнении.

IMPROOVMENT OF RISK MANAGMENT EVALUATION METHODS WHEN DESIGNING PROTECTED AUTOMATED SYSTEMS

O. Y. Kondrateva, D. V. Terin, E. V. Kondrateva

Directions for improving the assessment of risks arising from the operation of elements of automated systems were considered. The system is protected, but its “non-essential” functional elements can become unauthorized access channels. The number of channels and the probability of their occurrence corresponds to the expected behavior model of a potential intruder. A risk assessment model has been reviewed. The effectiveness of the model in the systems of segmentation, analysis and marketing of high-tech information and emulation of the processes for assessing the security of automated systems in a secure execution was ordered.

В настоящее время наблюдается экспрессивный рост внедрения цифровых технологий во все сферы жизнедеятельности при этом в условиях ограниченных ресурсно-временных возможностей процессов конструирования автоматизированных систем и их узлов возникает проблема управления рисками и совершенствования методов оценки информационной безопасности автоматизированных систем в защищенном исполнении [1,2]. С одной стороны, она является нетривиальной, а с другой - значительно влияет на эффективность мероприятий, направленных на поддержание информационной безопасности, в целом на систему управления рисками [3-5], процессов эксплуатации и себестоимость оценивания [6]. В качестве объекта исследования выступает комплекс управления подвижными объектами. Комплекс представляет собой автомати-

зированную систему управления с распределенной обработкой данных, имеющую открытый канал управления подвижным объектом [7]. Типовая схема объекта исследования представлена на рис. 1.

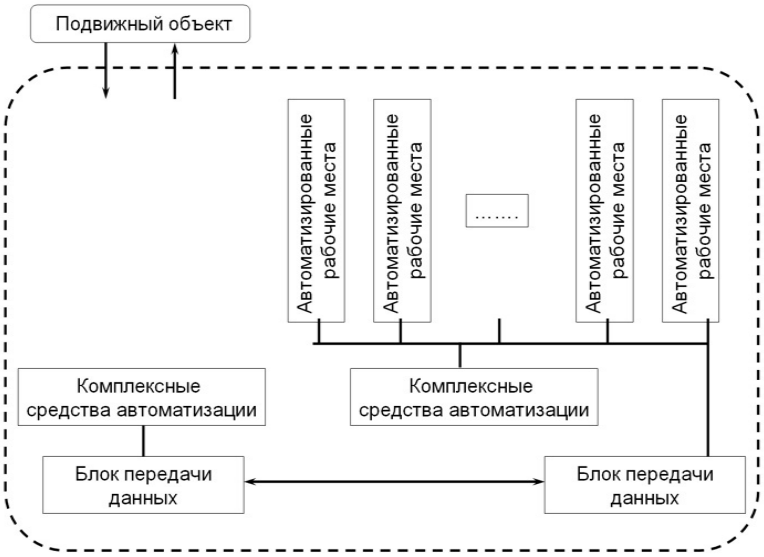

Рис. 1. Схема автоматизированной системы
в защищенном исполнении

В данной работе предлагается усовершенствованная модель оценки управления рисками информационной защищенности автоматизированной системы. Фундаментально модель базируется на показателях прочности контура безопасности и экспертном ранжировании вероятности существования каналов несанкционированного доступа (рис. 2).

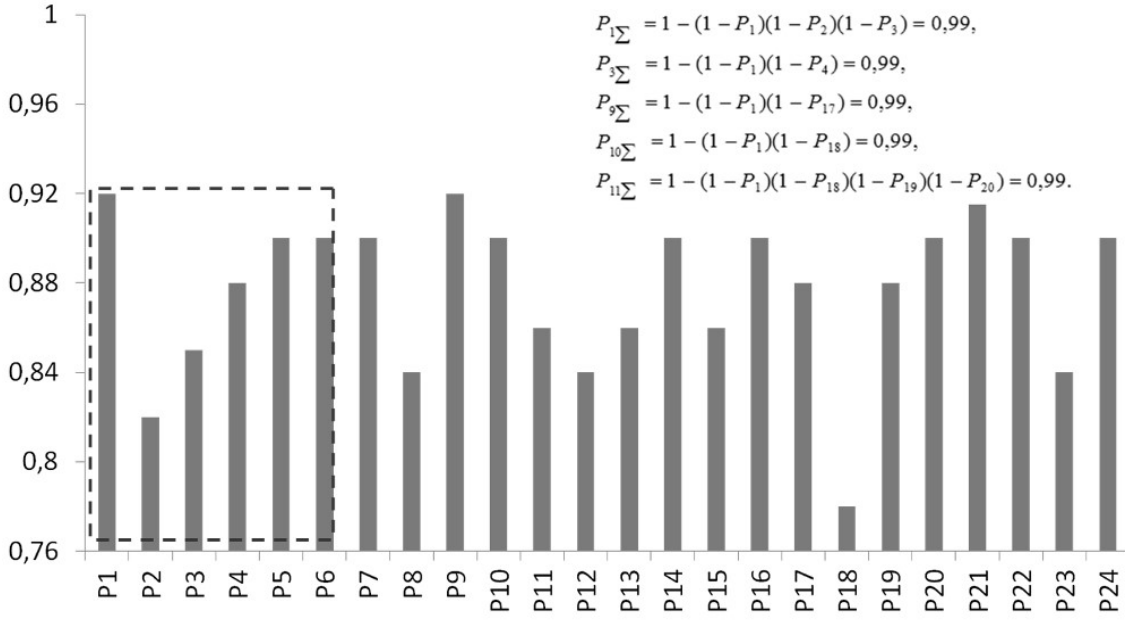

Рис. 2. Возможные каналы несанкционированного доступа

В соответствии с рис. 2 экспертно определялись вероятности существова-

ния следующих каналов несанкционированного доступа: Р1 - система контроля и разграничения доступа в помещения; Р2 - программно-аппаратный комплекс контроля входа в систему; Р3 - программа контроля и разграничения доступа к ПО и информации комплексных средств автоматизации; Р4 - система контроля ввода (вывода) аппаратуры в (из) рабочий контур обмена информацией; Р5 - средства стирания остатков информации; Р6 - средства наложения на остатки информации случайной последовательности символов и чисел; Р7 - средства уничтожения носителей секрет- ной информации; Р8 - учет и разграничение доступа к носителям; Р9- электронная идентификация носителей Р10 - шифрование информации; Р11 - резервирование информации с охраной ее копии; Р12 - учет, регистрация и разграничение доступа к документам; Р13 - учет, регистрация и разграничение доступа к носителям ПО; Р14 - верификация и контроль целостности ПО; Р15 - резервирование ПО с контролем доступа к его копии; Р16 - средства уничтожения носителей; Р17 - средства контроля и блокировки доступа к загрузке ПО; Р18 - система контроля вскрытия аппаратуры; Р19 - скрытая прокладка линий связи; Р20 - шифрование передаваемой информации; Р21 - программа контроля и разграничения доступа к информации комплекса средств автоматизации; Р22 - шифрование передаваемой информации; Р23 - организационные и технические средства защиты целостности канала связи с подвижным объектом; Р24 - средства снижения или зашумления уровня излучения и наводок информации на границе контролируемой зоны объекта автоматизации.

Уточнены интегрированные показатели «стабильной целостности» контролируемой и неконтролируемой оболочки защиты:

$$P_{ОЗК} = \min\{P_{1\Sigma}, P_2, P_{3\Sigma}, P_8, P_{13}, P_{16}, P_{9\Sigma}, P_{10\Sigma}, P_{21}\},$$

таким образом, оценка риска определялась вероятностью преодоления по пути с наибольшим значением этой вероятности и

$$P_{ОЗН} = \min\{P_5, P_6, P_7, P_{10}, P_{16}, P_{20}, P_{22}, P_{23}, P_{24}\},$$

минимизация рисков связана с преодолением неконтролируемых средств защиты. Усовершенствованная методология оценки управления рисками информационной защищенности автоматизированной системы показала свою эффективность в системах сегментирования, анализа и маркетирования наукоемкой информации [8] и эмуляции процессов оценки безопасности автоматизированных систем в защищенном исполнении [9]. Приведенная методология позволяет инструментально осуществлять разработку, конструирование, анализ, распределение и оценивать риски не только отдельных модулей защиты, но и всей системы в автоматизированных комплексах с сосредоточенной обработкой потоков больших данных как автономной системы и как элементов более сложной системы.

Работа выполнена при финансовой поддержке РФФИ в рамках научного проекта № 18-07-00752 а, проекта У.М.Н.И.К.-18 (б) договора № 13959ГУ/2019

СПИСОК ЛИТЕРАТУРЫ

1. ГОСТ Р 51583-2014 Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения. Введ. 2014-09-01. М. : Изд-во стандартов, 2014. 15 с.

2. ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Ч. 1. Введение и общая модель, Введ. 2013-12-01. М. : Изд-во стандартов, 2014. 58 с.

3. ГОСТ Р ИСО/МЭК ТО 19791-2008 Информационная технология. Методы и средства обеспечения безопасности. Оценка безопасности автоматизированных систем. Введ. 2009-10-01. М. : Изд-во стандартов, 2014. 122 с.

4. *Котенко И. В.* Методика выбора контрмер в системах управления информацией и событиями безопасности // Информационно-управляющие системы. 2015. № 3. С. 60-69.

5. *Шинкаренко А. Ф.* Методика оценивания защищенности информационно-телекоммуникационных узлов // Intellectual Technologies on Transport. 2016. № 1. С. 16-20.

6. *Коломеец М. В., Чечулин А. А., Дойникова Е. В.* Методика визуализации метрик кибербезопасности // Приборостроение. 2018. Т. 61. № 10. С. 873-880.

7. *Егоров С. В.* Оценка защищённости комплекса управления подвижными объектами на базе игровой модели // Научно-технический вестник информационных технологий, механики и оптики. 2006. № 25. С. 181-185.

8. Свидетельство о госрегистрации программы для ЭВМ 2016612523 РФ. Программный комплекс «Система сегментирования, анализа и маркетирования наукоемкой информации «КВРТ-1Г» / О. Ю. Кондратьева, Е. М. Ревзина, Д. В. Терин, Е. В. Кондратьева, С. Б. Вениг; Правообладатель СГУ им. Н. Г. Чернышевского. № 2015661026; заявл. 16.11.2015; зарегистр. 01.03.2016. опубл. 20.03.2016. 1 с.

9. Свидетельство о госрегистрации программы для ЭВМ 2017616859 РФ. Эмулятор процессов оценки безопасности автоматизированных систем в защищенном исполнении «ВИДЕМ-альфа» / В. Б. Байбурин, Д. В. Терин, М. А. Жилина; Правообладатель СГТУ им. Гагарина Ю.А. № 2017610234; заявл. 11.01.2017; зарег. 16.06.2017. опубл. 16.06.2017. 1 с.