УДК 004.9

МЕТОДИКА ОЦЕНКИ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Акперова А.А.

e-mail: dpo@iubip.ru

Иванова Е.Ю.

Главный государственный таможенный инспектор отдела документационного обеспечения Южного таможенного управления

e-mail: eyuiva@mail.ru

Аннотация: В статье рассматриваются вопросы анализа комплексной безопасности организации на примере частного вуза и таможенного управления Юга России. Оценивается эффективность сотрудников безопасности в разрезе обработки информационных атак. Даются рекомендации по выбору алгоритмов мониторинга безопасности.

Ключевые слова: аттестация программных средств, функциональное программирование, объектно-ориентированное программирование, хранение и обработка данных.

METHODOLOGY FOR ASSESSING THE INTEGRATED SECURITY OF THE ORGANIZATION

Akperova A.A.

Ivanova E.Yu.

Abstract: The article deals with the analysis of the complex security of an organization on the example of a private university and the customs department of the South of Russia. The effectiveness of security personnel in the context of processing information attacks is evaluated. Recommendations are given on the choice of security monitoring algorithms.

Keywords: software certification, functional programming, object-oriented programming, data storage and processing.

Исходя из особенностей комплексной безопасности вуза, соответствующий программного средства (ПС) включает анализ уровня безопасности и заданного перечня угроз безопасности, определяющих основных нарушителей (искусственные или естественные объекты). Следовательно, методика анализа безопасности должна учитывать:

– элементы оценки программного средства согласно заданным показателям и метрикам безопасности;

– элементы исследования возможных нарушителей;

– корректировку оценки в зависимости от изменения начальных

условий.

Начальные условия, применительно к процессу аттестации ПС, представляют собой перечень положений, выполняемых для обеспечения процесса исследования программного средства [1,2]:

– представление полной программной документации (эксплуатационной и конструкторской);

– представление исходных текстов программ;

– анализ источника получения программного средства;

– анализ условий предполагаемого применения;

– анализ модели ожидаемого поведения нарушителя;

– предоставление требований по безопасности.

Будем считать, что предоставление требуемых документов, включая исходные тексты программ, произведено в полном объеме. Анализ информации, обрабатываемой программным средством, на предмет ее ценности, сроков действия, а также особенностей предполагаемого размещения программного средства составляет основу для формирования типовых и индивидуальных требований по безопасности. Для критичных автоматизированных систем управления, обеспечивающих комплексную безопасность вуза, предварительный анализ условий получения и применения программного средства должен проводится с учетом того, что программное средство может выступать как в роли объекта разрушающего воздействия, так и в роли активного элемента информационного кибероружия [3].

Первоначальные условия также должны содержать анализ модели ожидаемого поведения нарушителя.

Для нарушителя, в качестве которого выступает человек, уже имеется достаточно хорошо разработанный аппарат защиты, основанный на моделях разграничения доступа [4]. Использование этих моделей позволяет создавать различные политики безопасности, реализуемые программно-аппаратными средствами.

Для нарушителя, в качестве которого выступают разрушающие программные средства (РПС) – специальные программные закладки, аппарат защиты находится еще в стадии формирования. Качественное постоянное изменение особенностей функционирования РПС привело к неадекватности описания некоторых моделей [5,6]. При оценке уровня безопасности необходимо дополнительно рассмотреть вопросы анализа свойств ПС, определяющих его способность к нанесению ущерба.

Основное содержание методики анализа безопасности программного средства, таким образом, составляет анализ потенциальных нарушителей и оценка уровня безопасности ПС. Указанные составные части методики представлены в виде: оценки уровня безопасности ПС; методика оценки уровня безопасности и формирование показателей и метрик безопасности ПС; анализа потенциальных нарушителей - методика идентификации программных закладок специального типа (система распознавания).

Решение задачи оценки уровня безопасности программных средств, прежде всего, связано с первоначальными условиями, которые должны быть определены в задании на проведение аттестации программного средства: условия получения программного средства; условия применения программного средства; комплекс мер по защите информации; перечень возможных каналов утечки информации.

После выполнения первоначальных условий проводится аттестация программного средства. Процесс оценки уровня безопасности ПС представляет собой оценку частных и интегрального показателей безопасности. Учитывая известные на данный момент методики оценки уровня защищенности ПС [7], оценки качества программных средств [8], общую структуру методики оценки уровня безопасности ПС можно представить в виде следующего алгоритма [3]:

Сбор исходных данных и заполнение информационных таблиц (СИД и ЗИТ) об объекте защиты, каналах утечки информации.

Процесс сбора исходных данных преследует цель предварительной

оценки информации, обрабатываемой ПС, на предмет ее ценности, сроков действия; возможных каналов утечки информации; угроз безопасности и целостности ПС; программно - аппаратной среды применения; роли и места испытуемого ПС в системе управления, уровня его изолированности в вычислительной системе.

СИД и ЗИТ о потенциальных нарушителях в ВС.

Основу второго этапа методики составляет сбор сведений о предполагаемых нарушителях: сущность, типы, функциональные возможности, особенности поведения, демаскирующие признаки, методы маскировки.

Ввод данных, характеризующих требования по безопасности.

СИД и ЗИТ ограничений на показатели и метрики безопасности согласно предоставленному перечню требований по безопасности ПС.

Расчет показателей безопасности ПС по заданным метрикам.

На данном этапе производится количественная и качественная оценка выбранных показателей безопасности.

Нормирование показателей в пределах единичной шкалы.

Подготовительный этап «свертки» частных показателей безопасности. Позволяет свести в единую расчетную процедуру качественные и количественные показатели безопасности ПС.

Определение интегрального показателя безопасности ПС.

На основе выбранного метода «свертки» частных показателей безопасности производится вычисление значения интегрального показателя и сопоставление его формализованному уровню безопасности ПС (одному из нормативных уровней безопасности ПС).

Основа методики – показатели и метрики безопасности, по которым возможно провести расчет уровня безопасности ПС.

Библиографический список

1. Akperov, I.G. Soft models of management in terms of digital transformation / I.G. Akperov, G.I. Akperov, T.V. Alekseichik [et al.]. – Rostov-on-Don: PEI HE SU (IMBL), 2019. – 188 p.

2. Алекперов И.Д. Информационная безопасность и защита информации в цифровой экономике: элементы теории и тестовые задания / И.Д. Алекперов [и др.]. – Ростов-на-Дону: Южный университет (ИУБиП), 2020. – 114 с.

3. Храмов, В.В. Нечеткий подход к проектированию экспертной системы по оценке защищённости программных средств кафедры вуза / В.В. Храмов, А.А. Чаушник // Ученые записки Института управления, бизнеса и права. Серия: Информационные технологии и управление. – 2012. – № 1. – С. 65-69.

4. Чернышев, Ю.О. Особенности агрегирования качественных признаков опорных ориентиров в системах технического зрения / Ю.О. Чернышев, В.В. Храмов // Известия ТРТУ. – 2001. – № 3(21). – С. 55.

5. Храмов, В.В. Защита информации в вычислительных системах : учебное пособие для вузов / В.В. Храмов, В.В. Садовов, А.Н. Трубников и др.. – М.: Пущинский научный центр Российской академии наук, 2002. – 192 с.

6. Akperov, G. I. Using soft computing methods for the functional benchmarking of an intelligent workplace in an educational establishment / G.I. Akperov, V.V. Khramov, A.A. Gorbacheva // Advances in Intelligent Systems and Computing (см. в книгах). – 2020. – Vol. 1095 AISC. – P. 54-60. – DOI 10.1007/978-3-030-35249-3_6.

7. Sakharova L.V., Stryukov M.B., Alekseichik T.V., Chuvenkov A.F., Akperov I.G. Application of fuzzy set theory in agro-meteorological models for yield estimation based on statistics // Procedia Computer Science. – 2017. – С. 820-829.

8. Akperov I.G., Khramov V.V. Development of instruments of fuzzy identification of extended objects based on the results of satellite monitoring // Advances in Intelligent Systems and Computing (см. в книгах). – 2019. – Т. 896. – С. 325-332.

9. Перспективы и возможности формирования системы экспертно-аналитического сопровождения международной деятельности российских университетов / А.А. Акишина, И.В. Антипина, А.И. Богуш [и др.]. – Москва: Издательский Центр РИОР, 2020. – 295 с. – DOI 10.29039/02044-9.

10. Belyaev, A. Research of tools for monitoring changes in natural and anthropogenic-transformed ecosystems / A. Belyaev [et al.] // IOP Conference Series: Earth and Environmental Science, Ussurijsk, –21 июня 2021 года. – Ussurijsk, 2021. – P. 022047. – DOI 10.1088/1755-1315/937/2/022047.

11. Системные проблемы надёжности, качества, математического моделирования и инфотелекоммуникационных технологий в инновационных проектах : коллективная монография / И.Г. Акперов, В.В. Храмов, О.А. Миронова [и др.]. – Москва: Национальный исследовательский университет "Высшая школа экономики", 2014. – 138 с. – ISBN 978-5-7598-1198-2.