УДК 004.056
DOI: 10.33764/2618-981X-2020-6-2-31-35

АВТОМАТИЗАЦИЯ ПРОЕКТИРОВАНИЯ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Амыртаа Кужугетович Монгуш
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, магистрант кафедры фотоники и приборостроения, тел. (996)545-07-00, e-mail: amyrtaakuzhuget@mail.ru

Игорь Николаевич Карманов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, кандидат технических наук, доцент, заведующий кафедрой физики, тел. (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

В связи с вступлением современного общества в информационный этап развития, информационная безопасность является одной из важнейших проблем современности. В данной статье рассматривается возможность автоматизации проектирования комплексной системы защиты информации. Одним из ключевых этапов проектирования системы защиты информации считается оценка текущего состояния системы информационной безопасности с помощью аудита. Аудит информационной безопасности позволяет выявить все уязвимые места в системе. Для автоматизации выявления уязвимостей исследуемого объекта рассматриваются сетевые сканеры. Применение сканеров позволяет решать задачи идентификации и анализа уязвимостей. Также рассмотрена схема автоматизация проектирования систем физической защиты. В заключении отмечены преимущества автоматизации проектирования системы защиты информации и приведены часто используемые программные средства и утилиты для автоматизации отдельных этапов проектирования систем защиты информации.

Ключевые слова: информационная безопасность, системы автоматизированного проектирования, аудит информационной безопасности, комплексная система защиты информации.

AUTOMATION OF COMPLEX INFORMATION SECURITY SYSTEMS DESIGN

Amyrtaa K. Mongush
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Graduate, Department of Photonics and Device Engineering, phone: (996)545-07-00, e-mail: amyrtaakuzhuget@mail.ru

Igor N. Karmanov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Ph. D., Associate Professor, Head of the Department of Physics, phone: (903)937-24-90, e-mail: i.n.karmanov@ssga.ru

Entry of modern society into the information stage of development wake, information security one of the most important problems of our time. The article discusses the possibility of automating the design of an integrated information security system. One of the key stages in the design of an information security system is the assessment of the current state of the information security system through audit. An information security audit allows identifying all vulnerabilities in the system. To automate the detection of vulnerabilities of the investigated object, network scanners are consid-

ered. The use of scanners allows solving the problems of identification and analysis of vulnerabilities. A scheme for automating the design of physical protection systems is also considered. In conclusion, the advantages of automating the design of an information protection system are noted, frequently used software tools and utilities for automating individual stages of the design of information protection systems are presented.

Key words: information security, information security audit, CAD systems, complex information security system.

Введение

При проектировании комплексных систем защиты информации (КСЗИ) нужно решить большое количество разнородных, часто слабоформализуемых задач. Чтобы снизить трудности и улучшить качество проектных решений, следует автоматизировать частные задачи, а также весь процесс проектирования КСЗИ. Автоматизация КСЗИ является актуальной проблемой, специфика которой заключается в том, что данная задача относится к классу слабоформализованных задач с неполной информацией.

В условиях слабоформализованных задач создание эффективной системы автоматизированного проектирования (САПР) представляется трудоемкой задачей, так как результат САПР однозначно зависит от сложившихся условий субъекта – проектировщика. Другими словами, сколько исполнителей проекта, столько и вариантов решений, и это влияет на объективность и совершенство проекта.

Аудит информационной безопасности

Защита информации реализуется с помощью фрагментарного или комплексного подходов, при этом фрагментарный подход обеспечивает противодействие строго определенным угрозам при определенных условиях, а комплексный – одновременное противодействие множеству угроз [1].

При проектировании КСЗИ одним из главных этапов является оценка текущего состояния системы информационной безопасности, то есть аудит информационной безопасности.

Аудит информационной безопасности позволяет выявить все уязвимые места в системе, а также понять, каким способом и через какие уязвимости злоумышленник может проникнуть в систему информационной безопасности. При проведении аудита приходится работать с большим объемом информации, поэтому иногда невозможно с помощью бумажных методик провести аудит. По этой причине многие организации, занимающиеся аудитом, применяют для аудита информационной безопасности различные программные средства анализа и управления рисками, которые построены по методике международных стандартов, таких как BS 7799 и ISO 17799. Также используют программные средства, направленные на анализ защищенности систем [2, 3, 4]. Средствами для анализа защищенности информационных систем могут быть сетевые сканеры.

Сетевые сканеры

Защищенность системы зависит от наличия в системе уязвимостей, через которые могут успешно осуществляться атаки [5]. С помощью современных сканеров можно обнаруживать сотни уязвимостей сетевых ресурсов, предоставляющих те или иные виды сетевых сервисов.

Сетевые сканеры – это программные или программно-аппаратные средства, позволяющие путем осуществления различных проверок (чаще всего это сканирование и зондирование) выявить уязвимость исследуемого объекта.

Применение сканеров позволяет решать следующие задачи [6]:

– идентификация доступных сетевых ресурсов;

– идентификация доступных сетевых сервисов;

– идентификация имеющихся уязвимостей сетевых сервисов;

– подготовка отчетных материалов, возможно, с описанием уязвимостей и рекомендациями по устранению.

Сканеры обычно выдают довольно общие рекомендации, и разработчик не всегда может быстро выяснить, как снизить уровень риска, и, самое главное, нужно ли это делать прямо сейчас или нет. Возможности сканера по анализу уязвимостей ограничены той информацией, которую могут представить ему доступные сетевые сервисы [7].

Системы автоматизированного проектирования систем физической защиты

Инженерно-техническая система защита информации (ИТСЗИ) является одним из основных компонентов комплексной системы защиты информации.

Проектирование ИТСЗИ является трудоемким слабоформализуемым процессом, реализация которого требует решения задач для оптимального выбора составных компонентов системы защиты. Для наиболее эффективного и наименее трудоемкого проектирования системы защиты рекомендуется использовать специализированную объектно-ориентированную систему автоматизированного проектирования [8].

В автоматизации проектирования системы защиты информации наиболее существенным считается этап моделирования объекта защиты.

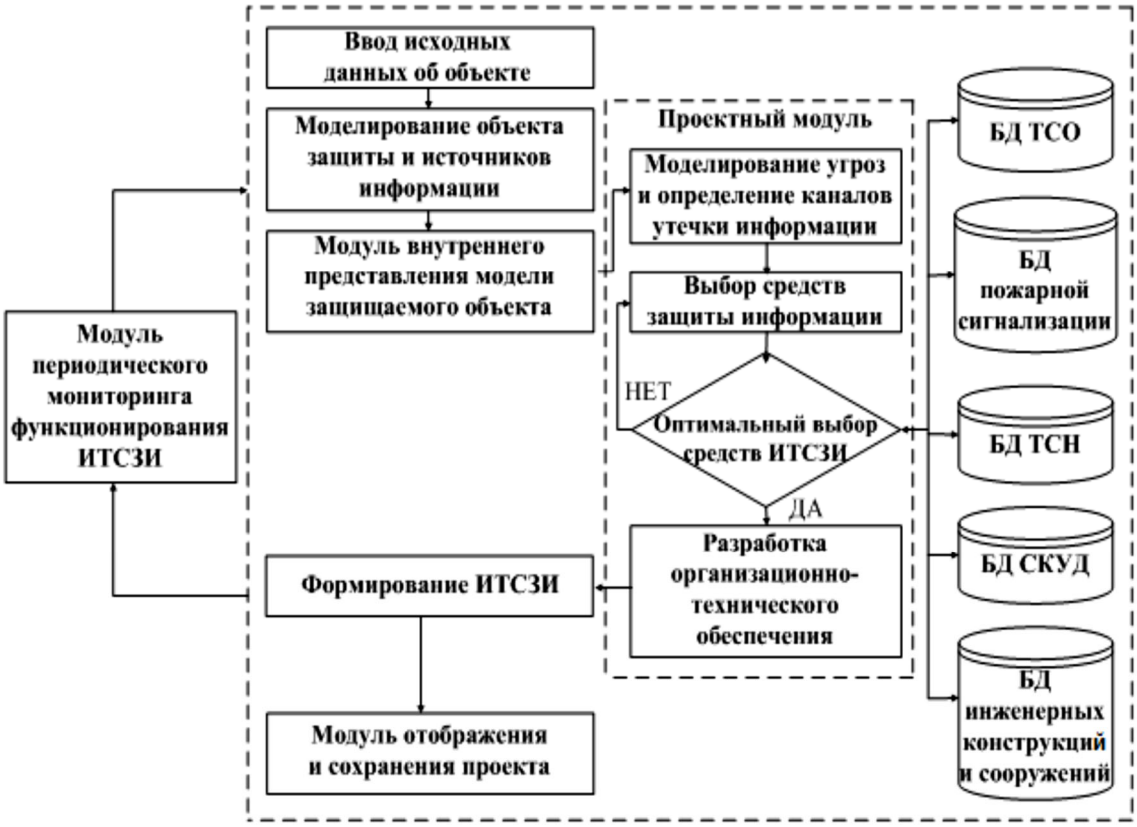
Модель, полученная после моделирования объекта защиты, передается в САПР ИТСЗИ в виде определенной структуры данных, которая содержит существенные свойства объекта защиты (например, площадь и этажность, выходы и входы объекта и т. д.) [9].

После завершения моделирования модели защищаемого объекта создается сама система защиты для защищаемого объекта.

На рисунке представлена структурная схема САПР ИТСЗИ.

Системы физической защиты включают в себя, как правило, охранно-пожарную систему, систему контроля и управления доступом, систему видеонаблюдения и т. п.

По принципу комплексного (системного) подхода системы защиты информации каждый компонент системы физической защиты в САПР ИТСЗИ проектируется в виде отдельного модуля [10].



Структурная схема системы автоматизированного проектирования инженерно-технической системы защиты информации

Система автоматизированного проектирования системы технической защиты информации (САПР СТЗИ) состоит из нескольких модулей [10].

Используя модуль ввода данных об объекте, вводятся данные о текущем состоянии системы защиты.

Для получения модели объекта используется модуль моделирования объекта защиты и определения источников информации.

Модуль внутреннего представления модели защищаемого объекта преобразует исходные данные в единый формат, доступный для всех модулей САПР ИТСЗИ.

В проектном модуле определяются все возможные угрозы и каналы утечки информации (модель угроз). Далее с помощью модули выбора средств защиты информации подбираются методы и средства защиты информации из базы данных (БД). БД состоит из БД технических средств охраны (ТСО), пожарной сигнализации, телевизионных систем видеонаблюдения (ТСН), систем контроля и управления доступом (СКУД) и инженерных конструкций и сооружений.

Модуль оптимального выбора средств ИТЗИ используется для оптимального выбора средств физической защиты информации.

Для разработки правовой и технической документации по проекту используется модуль разработки организационно-технического обеспечения.

Модуль формирования ИТСЗИ формирует конечный проект ИТСЗИ.

Модуль сохранение проекта используется для документирования, сохранения и дальнейшего использования результатов проектирования ИТСЗИ.

Модуль периодического мониторинга функционирования ИТСЗИ используется для обеспечения периодического контроля эффективности средств защиты и соответствия их требованиям информационной безопасности.

Заключение

Автоматизация проектирования КСЗИ позволяет специалистам по информационной безопасности создать систему защиты на объекте в кратчайшие сроки, используя минимум финансовых ресурсов.

В практике при автоматизации проектирования комплексных систем защиты информации часто применяются программные средства и утилиты для автоматизации отдельных этапов проектирования КСЗИ, например, широко известны и применяются такие системы как «Кондор», «Авангард» и «Гриф».

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1 Ваулин С. С. Безопасность автоматизированных систем : методические указания – Екатеринбург: УрФУ, 2011. – 23 с.

2 Аверченков В. И. Аудит информационной безопасности органов системы государственного и муниципального управления : монография – Брянск : БГТУ, 2008. – 126 с.

3 Домарев В. В. Безопасность информационных технологий. Системный поход. – Киев : ООО ТИД «ДС», 2004. – 992 с.

4 Луценко В. М. Автоматизация проектирования комплексных систем защиты информации с использованием средств поддержки принятия решений // Научно- практический журнал «Захист інформації». – 2012. – № 3 (22). – С. 1–6.

5 Аверченков В. И. Аудит информационной безопасности : учеб. пособие для вузов. – М. : ФЛИТА, 2016. – 269 с.

6 Черемных В. Сканеры уязвимости [Электронный ресурс]. – Электрон. дан. – М., 2017. – Режим доступа: https://it-black.ru/skanery-uyazvimostey/ – Загл. с экрана. (дата обращения 12.02.2020)

7 Марков А. С., Миронов С. В., Цирлов В. Л. Выбор сетевого сканера для анализа защищенности сети // BYTE Россия. – 2005. – № 6. – С. 67–70.

8 Аверченков В. И. Методы и средства инженерно-технической защиты информации. – Брянск : БГТУ, 2012. – 187 с.

9 Аверченков В. И., Рытов М. Ю. Автоматизация проектирования комплексных систем защиты информации // Информация и безопасность. – 2007. – № 4. – С. 582– 584.

10 Еременко В. Т. Комплексные системы защиты информации предприятия : учеб. пособие. – Орел : ФГБОУ ВО «Орловский государственный университет имени И. С. Тургенева», 2016. – 115 с.