Введение

Проблемы безопасности инфокоммуникационных систем затрагивают множество составляющих — от защиты локальных сетей, в том числе беспроводных, до внедрения методов и средств защиты на мобильные устройства и Интернет-ресурсы. Важно не только обеспечить постоянную защиту инфокоммуникационной системы и предотвратить утечку конфиденциальной информации, но и реализовать непрерывный аудит событий безопасности, включающий подсистемы идентификации и аутентификации, резервного копирования и так далее.

Необходимо проектировать системы, которые могут адаптироваться к различного рода атакующим воздействиям злоумышленника, наиболее опасным из которых является нарушение целостности и доступности сетевых ресурсов, поэтому большой интерес представляют методы и технологии противодействия атакам класса «отказ в обслуживании». Также стоит учитывать наличие уязвимостей у тех технологий, которые используются для обеспечения безопасного информационного взаимодействия. Наиболее ярким примером этого являются проблемы с безопасностью протокола HTTPS и его составляющих, которые достаточно широко используются в инфокоммуникационных системах.

Каждая глава учебного пособия посвящена решению представленных выше проблем в области информационной безопасности инфокоммуникационных систем. Для этого в нем приведен набор методов, технологий и средств, позволяющий противодействовать угрозам различным составляющим инфокоммуникационной системы. Также представлены примеры, иллюстрирующие обеспечение безопасного информационного взаимодействия в таких системах.

Безопасность локальных сетей, обычно включающих в себя беспроводной сегмент с технологией Wi-Fi, является основой при проектировании защищенных инфокоммуникационных систем. Отсутствие надежной защиты беспроводного соединения несет серьезную угрозу всем устройствам такой сети: от серверов и рабочих станций до интегрированных в нее мобильных устройств. Именно поэтому в первой главе уделено внимание технологии WPA3, внедрение которой в ближайшие годы существенно улучшит безопасность беспроводных сетей стандартов IEEE 802.11.

SIEM-системы широко применяются для аудита различных составляющих инфокоммуникационной системы, что нашло отражение во второй главе данного пособия. Одной из таких составляющих является подсистема идентификации и аутентификации пользователей, рассмотренная в третьей главе. В ней подробно описаны биометрические методы аутентификации, приведены их достоинства и недостатки, а также варианты реализации единой аутентификации на нескольких Интернет-ресурсах, как правило, основанной на использовании пароля, что также отображено в главе.

Особую роль в инфокоммуникационной системе играет протокол HTTPS, который используют многие прикладные процессы и сервисы. Однако у него есть несколько слабых мест, на которые может быть успешно реализована атака. Методам и технологиям противодействия этим атакам отведена бóльшая часть четвертой главы.

В пятой главе рассмотрены модели использования мобильных устройств сотрудниками организации в контексте обеспечения информационной безопасности. В ней приведены угрозы информационной безопасности мобильных устройств при их интеграции в сеть предприятия, а также технологии управления ими и обеспечения их защиты.

Шестая и седьмая главы посвящены широко распространенным средствам обнаружения уязвимостей и противодействия сетевым атакам — сканерам уязвимостей, межсетевым экранам и системам предотвращения утечки информации. Межсетевые экраны широко применяются для защиты инфокоммуникационных систем от атак класса «отказ в обслуживании», разновидности и методы противодействия которым представлены в восьмой главе.

Без надежного и безопасного хранения данных нельзя в полной мере обеспечить конфиденциальность и целостность информации в инфокоммуникационной системе. В девятой главе рассмотрена структура системы хранения данных, предъявляемые к ней требования и технологии резервного копирования. Особое внимание уделено технологии резервного копирования путем децентрализованного распределения файлов по устройствам с использованием peer-to-peer системы хранения данных.

Последняя глава содержит наиболее распространенные и актуальные уязвимости веб-ресурсов, приводящие к реализации атак. В ней приведены методы, технологии и средства защиты от таких атак с учетом широкого применения спецификации HTML5.