ПРОЕКТИРОВАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

А.В. Федосеев

В последнее время различные исследователи все чаще к факторам общественного производства (помимо труда, земли, капитала и предпринимательства) относят информацию. Это говорит об изменившемся положе-

нии информации в современных условиях хозяйствования: она занимает все больший удельный вес среди экономических благ, созданных современными хозяйственными системами, и является важным условием принятия рациональных решений.

Можно утверждать, что информация является одним из важнейших активов современного предприятия. Поэтому ее разглашение, утрата или недоступность может иметь серьезные неблагоприятные последствия. Например, недоступность или повреждение информации в результате сбоя в работе вычислительного и сетевого оборудования, может привести к нарушению производственного цикла, недоверию со стороны клиентов и потере рыночной конкурентоспособности. Кроме того, в процессе хозяйствования организаций возникают также и другие риски, в том числе связанные с передачей информации третьим лицам или использованием важной информации инсайдерами в целях мошенничества в связи со сделками с ценными бумагами.

Поэтому возникает необходимость в максимальном повышении защищенности организации от сбоев и потери информации, а именно, в проектировании комплексной системы защиты информации. При этом, необходимо отметить, что понимание информационных угроз у разных организаций отличается. Например, для промышленных предприятий основная опасность заключается в хищении конфиденциальной конструкторской и технологической документации, для банков – в несанкционированном вторжении в базы данных финансовых транзакций, а для поставщиков Интернет-услуг главное – обеспечить работоспособность и доступность каналов. Кроме того, выбор систем защиты информации зависит и от размеров организации, ее платежеспособности. Поэтому главной целью проектирования подобной защиты является разработка оптимальной комплексной системы по используемым технологиям и по наилучшему соотношению цены к получаемой степени безопасности. Максимизация эффективности комплексной системы защиты информации должна достигаться за счет качественно реализованных решений ее компонентов, функционирующих как единый комплекс и имеющих централизованное управление.

Комплексные системы защиты информации могут включать в себя следующие подсистемы:

- защиты от несанкционированного доступа;
- антивирусной защиты;
- управления правами доступа и учетными записями;
- криптографической защиты;
- межсетевого экранирования (статические пакетные межсетевые экраны, динамические межсетевые экраны и межсетевые экраны уровня приложений);
- контроля эффективности средств защиты информации и др.

При этом контроль эффективности средств защиты информации является важной функцией, необходимой для достижения целей информационной безопасности и включает в себя проверку соответствия эффективности работ по защите информации установленным требованиям и/или нормам эффективности защиты информации.

Средства подсистемы позволяют облегчить и автоматизировать мероприятия, выполняемые в рамках процесса контроля эффективности защиты информации:

- анализ уязвимостей сетевой и системной инфраструктуры – деятельность по выявлению уязвимостей в программно-аппаратном обеспечении на основе всесторонних или выборочных тестов сетевых сервисов, операционных систем, прикладного программного обеспечения, маршрутизаторов, межсетевых экранов и т.п.;
- анализ уязвимостей СУБД или web-приложений – используется для выявления уязвимостей характерных исключительно для баз данных или web-приложений и web-сервисов;
- контроль политик безопасности – деятельность по контролю выполнения правил политики безопасности. Это позволяет в любой момент времени иметь актуальную информацию об элементах информационной системы, состояние которых нарушает политику безопасности, и оперативно устранять несоответствия.

Проектирование комплексной системы защиты информации должно включать в себя, во-первых, проведение предпроектного обследования, а во-вторых, техно-рабочее проектирование системы защиты информации.

Так, проведение предпроектного (специального) обследования подразумевает:

1. Сбор и уточнение данных о локальной вычислительной сети (ЛВС) и осуществляемых видах деятельности (технологических операций обработки информации).
2. Оценка качества функционирования ЛВС и осуществляемых видов деятельности.
3. Определение и проведение необходимого объема исследовательских работ.
4. Разработку концепции построения ЛВС, удовлетворяющего требованиям Специальных требований и рекомендаций по технической защите конфиденциальной информации.
5. Оформление отчёта о выполненной работе.

Техно-рабочее проектирование системы защиты информации должно проводиться с соблюдением требований действующего законодательства Российской Федерации и включает в себя:

1. Разработку проектных решений по системе и её элементам;
2. Разработку проектной документации на систему и её элементы;

3. Разработку и оформление в рамках проектных решений документации на поставку изделий для доукомплектования системы;

4. Разработку заданий на проектирование системы и ее частей;

5. Разработку рабочей документации на систему и её части (в соответствии со СНиП 11-01-95 «Инструкция о порядке разработки, согласования, утверждения и составе проектной документации на строительство предприятий, зданий и сооружений»).

Проектирование, организация и применение систем защиты информации фактически связаны с неизвестными событиями в будущем и поэтому всегда содержат элементы неопределенности. Кроме того, присутствуют и другие причины неоднозначности, такие как недостаточно полная информация для принятия управленческих решений или социально-психологические факторы. Поэтому, например, этапу проектирования системы защиты информации естественным образом сопутствует значительная неопределенность. По мере реализации проекта ее уровень снижается, но никогда эффективность системы защиты информации не может быть адекватно выражена и описана детерминированными показателями. Поэтому для ответа на вопрос, в какой мере система защиты информации обеспечивает требуемый уровень безопасности, необходимо оценивать эффективность системы защиты информации показателями, носящими вероятностный характер. А содержательные результаты по оценке эффективности комплексных систем защиты информации могут быть получены при системном подходе, более того, его обязательность прямо вытекает из ГОСТ Р50922-96 [1].

Библиографический список

1. ГОСТ Р 50922-96 Государственный стандарт Российской Федерации: Защита информации: Основные термины и определения / Издание официальное, Госстандарт России. – М., 1996.