вера. В 87 % продуктов специалистами была выявлена недостаточная защита пакета приложения и его компонентов, в 78 % – отсутствие проверок наличия несанкционированного привилегированного доступа к мобильному устройству.

О НЕКОТОРЫХ НАПРАВЛЕНИЯХ РАЗРЕШЕНИЯ ПРОБЛЕМ, ВОЗНИКАЮЩИХ ПРИ ПОСТРОЕНИИ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИЯХ СОЮЗНОГО ГОСУДАРСТВА

В. В. БЕЗМЕН, Л. Л. УТИН

Непрерывное развитие информационных технологий (ИТ), разработка и внедрение нового телекоммуникационного оборудования, совершенствование возможностей технических средств, используемых злоумышленниками для нанесения ущерба информационным ресурсам, приводят к необходимости постоянного совершенствования созданной системы защиты информации (СЗИ).

Современная нормативно-правовая база в области информационной безопасности (ИБ) определяет СЗИ как комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.

Согласно действующим нормативным документам процесс создания СЗИ в информационных системах (ИС) включает целый комплекс мероприятий. Однако, указанные документы предоставляют в большей степени теоретические принципы создания системы обеспечения ИБ, в то время как практическое внедрение и эффективное использование комплекса организационных и технических средств ЗИ за счет многообразия существующих продуктов и услуг ИБ представляют собой трудную задачу.

Анализ подходов, принятых к формированию стандартов в ряде зарубежных стран, показывает, что очень часто эти стандарты носят рекомендательный характер и не претендуют на полный охват всевозможных вызовов и угроз. Положение усугубляется и тем, что из-за огромного количества всевозможных угроз информационной безопасности, высокой динамики их появления, особенностей, присущих конкретным предприятиям, достаточно сложно осуществить их каталогизацию с формальным описанием признаков проявления.

Следует отметить, что аналитическими исследованиями угроз информационной безопасности как в Республике Беларусь, так и Российской Федерации занимается небольшое количество организаций. Одной из наиболее известных является аналитический центр компании InfoWatch, предоставляющий ежегодные отчеты об исследовании утечек информации, распространение которой ограничено.

Так, результаты анализа наглядно демонстрируют увеличение числа утечек информации. Большинство утечек в 2014 г. пришлось на три основных канала: интернет (35 %), бумажные документы (18 %) и кража/потеря оборудования (16 %).

Эксперты уверены, что большая часть совершаемых компьютерных преступлений остается не обнаруженными. Это говорит о высокой степени актуальности решения проблемы создания и использования СЗИ на предприятиях различных отраслей деятельности.

Многолетний практический опыт деятельности в области ЗИ показал, что для любого предприятия союзного государства при построении СЗИ целесообразно рассматривать следующие подсистемы:

- подсистему аутентификации и авторизации;
- подсистему контроля доступа и защиты от НСД;
- подсистему защиты сетевой инфраструктуры (межсетевого экранирования);
- подсистему обнаружения и предотвращения атак;

• подсистему криптографической защиты информации;
• подсистему противодействия вредоносному программному обеспечению;
• подсистему управления информацией о событиях ИБ, корреляции, мониторинга и анализа событий;
• подсистему контроля эффективности технических средств защиты информации.

Исходя из потребностей каждой организации данные подсистемы могут быть объединены в одни средства защиты, либо функции одной подсистемы могут выполняться средствами параллельно из других подсистем; данное деление было определено по выполняемым функциям защиты от определенного вида угроз.

В докладе раскрываются проверенные на практике пути выбора конкретных вариантов построения и последующей эксплуатации СЗИ на информационных системах различных предприятий и организаций. Детально рассматриваются варианты ряда подсистем. Приводятся варианты технического решения с использованием аппаратных и программных средств, в том числе и разработанных на государственном предприятии «НИИ ТЗИ».

Авторами показано, что из-за стремительного развития рынка и продуктов в области ИБ отделы технической ЗИ, отвечающие за безопасность на своем предприятии, должны:

• своевременно корректировать документацию, сопровождающую СЗИ на каждом этапе ее эксплуатации;
• осуществлять непрерывный мониторинг состояния всех средств защиты, используемых на предприятии;
• следить за уровнем защищенности циркулирующей информации.

Своевременное выявление и нейтрализация угроз информационной безопасности на предприятиях союзного государства возможна при непрерывной оценке эффективности используемых средств ЗИ. При этом в последние годы НПА существенно ужесточены требования ко времени реакции СЗИ на появление новых угроз информационной безопасности предприятий.

В заключение следует отметить, что НИИ ТЗИ является ведущим предприятием в области сертификации и разработки средств защиты Республики Беларусь, в котором не только разрабатываются и доводятся до серийного изготовления новейшие средства ЗИ, но и осуществляется тестирование практически всех новейших продуктов информационных технологий, учет которых необходим в режиме, приближенном к реальному времени.