(КВО) отраслевых инфраструктур, включающие:

– обеспечение безопасности функционирования КВО и жизнедеятельности населения, в том числе, в условиях чрезвычайных ситуаций;

– предупреждение и локализация угроз техногенного характера, совершенствование систем мониторинга и прогнозирования чрезвычайных ситуаций техногенного характера;

– создание эффективных систем защиты КВО;

– недопущение организации и активизации террористической деятельности в отношении КВО инфраструктуры страны; разработка и реализация правовых и экономических средств защиты КВО.

Законодательство государств-участников Союзного государства устанавливает основные направления защиты информации на КВО:

– обеспечение конфиденциальности информации о критических активах, являющихся главными объектами диверсий и саботажа, информации, хранящейся в архивах и автоматизированных информационных системах организационного управления.

– обеспечение целостности и доступности информации (данных), циркулирующей в системах контроля и управления, созданных на базе вычислительной техники (компьютерных систем), важных для безопасности КВО.

Анализ национальных нормативных и нормативных технических актов государств-участников Союзного государства выявил подходы в области защиты информации и обеспечения информационной безопасности КВО, их согласованность и различия, что потребовало разработки соответствующего документа в рамках Союзного государства – Концепции обеспечения информационной безопасности КВО.

АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УСТРОЙСТВ «ИНТЕРНЕТА ВЕЩЕЙ» (INTERNET OF THINGS)

В.Ф. Кулиш, Т.В. Борботько

Широкое распространение сетевых технологий и облачных вычислений, а также внедрение протокола IPv6 привело к появлению большого числа устройств Интернета вещей, подключенных к сети Интернет. Интернет вещей - концепция вычислительной сети физических устройств, оснащенных встроенными технологиями для взаимодействия друг с другом посредством сети Интернет. Осенью 2016 года стало известно о появлении ботнета Mirai, который на тот момент включал в себя 400 тыс. устройств Интернета вещей. Создатель ботнета предоставил в открытом доступе исходный код, использовавшийся для внедрения вредоносных программ. Это позволило исследователям изучить его архитектуру и выявить основные векторы атак.

1. Применение стандартных имен пользователей и паролей для аутентификации в панелях управления устройств. В коде модуля для заражения устройств был обнаружен список с именами пользователей и паролями. Для заражения ботнет использовал сетевой протокол telnet, который позволяет удаленно выполнять команды на устройстве.

2. Использование уязвимостей в веб-приложениях для управления параметрами устройства. Для атаки использовалась уязвимость в обработке данных, полученных по протоколу CWMP, который применяется поставщиками услуг подключения к сети Интернет для удаленного управления абонентским оборудованием.

Основными проблемами обеспечения безопасности являются небезопасная базовая конфигурация устройств, а также не реализованный механизм обновления этих устройств. Данные по распространенности устройств свидетельствуют о том, что устройств Интернета вещей с каждым днем будет становиться все больше. Поэтому проблема их безопасности является весьма актуальной.

БЕЗОПАСНОСТЬ ИСПОЛЬЗОВАНИЯ БИОМЕТРИЧЕСКИХ СКАНЕРОВ В МОБИЛЬНЫХ УСТРОЙСТВАХ

И.И. Лабаревич

На данный момент самое распространенное применения биометрии в мобильных устройствах – это сканер отпечатка пальцев. На телефонах под управлением ОС IOS это Touch

ID, а на телефонах под управлением ОС Android это Fingerprint.

Алгоритмы реализации данной технологии в этих системах разные. Заранее скажу, что сканер отпечатков пальца на IOS на порядок лучше и гораздо труднее поддается взлому, чем аналогичная технология на Android-телефонах. Физически, эти сканеры реализованы по-разному, а также имеют разные способы шифрования самих сканов.

В телефонах компании Apple сканированный отпечаток пропускается через хеш-функцию и сохраняется в Secure Enclave – защищенном от доступа извне микрокомпьютере.

В телефонах под ОС Android до 6 версии операционной системы были даже такие казусы, как хранение сканов в памяти телефона, в незашифрованном виде, в общедоступной папке. С выходом Android 6.0 в Google не только разработали собственный API для аутентификации по отпечаткам пальцев, но и обновили Compatibility Definition Document, которому обязаны следовать все производители, желающие сертифицировать свои устройства для установки сервисов Google (это очень важный момент, о нем чуть позже).Было выпущено сразу два референсных устройства: Nexus 5X и Nexus 6P. В них – и неотключаемое шифрование раздела данных, и правильная реализация датчиков отпечатков, получившая название Nexus Imprint.

Сравнить безопасность Touch ID с ситуацией в мире Android не получится: если у Apple устройств единицы, то смартфонов на Android, наоборот, слишком много. В них могут использоваться самые разные датчики, основанные на разнообразных технологиях (от емкостных и оптических до ультразвуковых). Для разных датчиков подбирают разные технологии обхода. К примеру, для Samsung Galaxy S6 вполне срабатывает финт с разблокированием телефона моделью пальца, напечатанной на 3D-принтере из самого обычного пластика (с Apple Touch ID такой простой трюк не пройдет; для печати нужно будет использовать материал, обладающий особыми свойствами). Некоторые другие устройства легко обманываются распечатанными с высоким разрешением картинками. А вот сравнение с Nexus Imprint вполне имеет смысл. В Nexus 5X и 6P Google использовал образцово-показательный подход к безопасности. Это и неотключаемое шифрование раздела данных, и грамотная интеграция датчиков отпечатков, да и сами датчики выбраны не абы как. В устройствах сторонних производителей могут использоваться недостаточно безопасные датчики, могут зиять откровенные дыры в безопасности (несмотря на формальное соответствие требованиям Android Compatibility Definition). Дактилоскопическая аутентификация – не панацея. Ее основное предназначение не в том, чтобы сделать более безопасным конкретно твое устройство, а в том, чтобы снизить неудобства, связанные с безопасной блокировкой телефона, и таким образом убедить основную массу пользователей все-таки блокировать свои устройства.

АУДИТ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ ЭЛЕКТРОННОГО БИЗНЕСА

Л.М. Лыньков, В.С. Князькова

Организация электронного бизнеса (ОЭБ) с точки зрения технического обеспечения представляет собой единое информационное пространство, интегрирующее в себя функциональные области маркетинга, производства, финансов, кадров и т.п. Комплексная оценка информационной инфраструктуры ОЭБ, в частности ее информационной безопасности (ИБ) организуется через аудит системы ИБ. К основным особенностям проведения аудита ИБ ОЭБ можно отнести следующие. Во-первых, ОЭБ представляет собой сложную и многоуровневую систему, включающую множество подсистем (функциональные области, например, финансы и маркетинг) и надсистем (например, контролирующие органы). Во-вторых, средой функционирования ОЭБ является сеть Интернет, использование которой привносит дополнительные риски для организации в силу ее общедоступности. В-третьих, в ОЭБ на первый план выходит обучение всех без исключения сотрудников как минимум основам ИБ. Согласно исследованию, проведенному в 2014 г. компанией Ernst & Young, 33% респондентов назвали именно персонал одним из основных источников угроз ИБ.

Обычно ОЭБ осуществляет свою деятельность через интернет-сайт. В таком случае при аудите системы ИБ необходимо оценить такие аспекты, как соответствие контента и