регламентирующих построение и функционирование систем видеонаблюдения:

– различия в терминологии;

– однозначно не регламентированы требования к защите информации / видеоинформации, включая ее защиту от модификации;

– не указаны категории объектов на которых допускается скрытая установка систем видеонаблюдения;

– имеется двойственность требований в обеспечении резервного электропитания;

– различие требований к составу охранной телевизионной системы / системы видеонаблюдения;

– несоответствие наименований и детализированного описания (параметр/показатель) уровней различения;

– отсутствуют единые требования к сертификации / подтверждению соответствия составных элементов системы видеонаблюдения;

– отсутствуют требования к молниезащите систем видеонаблюдения;

– не описаны вопросы организации передачи видеоинформации при создании и применении систем видеонаблюдения с использованием радиоканальной направляющей среды.

На основании изложенного выше можно сделать вывод, что создание нормативно-правовой базы, регламентирующей вопросы нормативно-правового, организационно-технического и технического обеспечения построения и функционирования РСМОБ является сложной задачей и потребует приведения в соответствие значительного числа действующих НПА/ТНПА Республики Беларусь в отрасли систем видеонаблюдения.

О ПРОЕКТАХ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ СОЮЗНОГО ГОСУДАРСТВА

Э.П. Крюкова, А.А. Ковалевский

Целью работы, выполненной в рамках Союзной программы ((шифр «Норма»), было исследование особенностей, разработка организационно-правовых основ формирования систем и механизмов обеспечения информационной безопасности субъектов и критически важных объектов Союзного государства, защиты информации, не составляющей государственные секреты, об этих субъектах и объектах. Анализ законодательства Республики Беларусь и Российской Федерации в области обработки, использования и защиты сведений, составляющих служебную информацию ограниченного распространения, персональную информацию, коммерческую тайну, информацию на критически важных объектах показал, что при наличии согласующихся положений правовых актов имеются и существенные разночтения, и пробелы в механизмах защиты прав владельцев (собственников) такой информации и систем ее обработки. Разработаны проекты пяти нормативных правовых актов Союзного государства: «О порядке обработки, использования и защиты персональных данных», «О порядке использования и защиты сведений, составляющих коммерческую тайну», «О служебной информации ограниченного распространения в Союзном государстве», «О порядке использования и защиты служебной информации ограниченного распространения Российской Федерации и Республики Беларусь», «Концепция информационной безопасности критически важных объектов Союзного государства». При разработке этих документов использован современный мировой, в частности, европейский опыт правового регулирования отношений в рассматриваемых областях. Разработанные документы содержат положения, устанавливающие механизмы правового регулирования взаимоотношений государств-участников Союзного государства в области защиты критически важной информации, а также правоотношений субъектов государств-участников Союзного государства, и могут быть использованы для совершенствования национального законодательства.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КРИТИЧЕСКИХ ВАЖНЫХ ОБЪЕКТОВ

Э.П. Крюкова, В.А. Филипович

В законодательстве государств-участников Союзного государства нашли отражение основные задачи обеспечения информационной безопасности критически важных объектов

(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