функциональными задачами информационных систем. Для эффективного решения проблем информационной безопасности необходима комбинированная реализация программных и аппаратных средств, которые поддерживают современные криптографические алгоритмы, обеспечивающие решение подавляющего большинства проблем безопасности, таких как аутентификация, шифрование данных, контроль целостности, электронная цифровая подпись; и должны поддерживать гибкость применения и высокую масштабируемость решений.

Литература

1. Статистические данные за 2016 год // МВД Республики Беларусь. URL: http://mvd.gov.by/main.aspx?guid=3311 (дата доступа: 17.05.2017).

ИЗМЕНЕНИЕ В СТАНДАРТ СТБ 34.101.8-2006 ПРОВЕДЕНИЕ ИСПЫТАНИЙ

Д.И. Жукова, Д.В. Шуляк

Одним из основных изменений в СТБ 34.101.8-2006 является расширение классификации ПСЗВВП и АПС. В новой редакции стандарта добавляются следующие типы ПСЗВВП и АПС:

ПСЗВВП и АПС четвертого типа в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку пакетов сетевого трафика и обезвреживание обнаруженных ВП;

ПСЗВВП и АПС пятого типа в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку файлов данных, передаваемых по почтовым протоколам, и обезвреживание обнаруженных ВП;

ПСЗВВП и АПС шестого типа в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку элементов объекта ИТ на наличие ВП, выявление вредоносного воздействия и обезвреживание обнаруженных ВП;

ПСЗВВП и АПС седьмого типа в течение работы объекта ИТ должны обеспечивать в реальном масштабе времени автоматическую проверку файлов данных, передаваемых по сети, и обезвреживание обнаруженных ВП;

ПСЗВВП и АПС восьмого типа после запуска по запросу пользователя должны обеспечивать проверку элементов объекта ИТ на наличие ВП и обезвреживание обнаруженных пассивных и активных ВП.

Ко всем типам ПСЗВВП и АПС стандарт устанавливает детальные требования. Уточненная классификация позволит улучшить качество СЗИ допускаемых к распространению на рынке Республики Беларусь.

Литература

1. СТБ 34.101.8-2006 «Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования».

2. Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 17 декабря 2013 г. № 94 «О перечне технических нормативных правовых актов, взаимосвязанных с техническим регламентом ТР 2013/027/BY».

3. Технический регламент Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/BY).

ОЦЕНКА НОРМАТИВНО-ПРАВОВОГО ОБЕСПЕЧЕНИЯ СОЗДАНИЯ РЕСПУБЛИКАНСКОЙ СИСТЕМЫ МОНИТОРИНГА ОБЩЕСТВЕННОЙ БЕЗОПАСНОСТИ

Ю.А. Ковалевич, И.В. Елсаков, А.В. Шкробот

При проектировании и построении республиканской системы мониторинга общественной безопасности (РСМОБ) для конкретных целевых групп объектов в рамках профильного сегмента обеспечения общественного порядка существует ряд противоречий в нормативно-правовых, организационно-технических и технических вопросах,

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