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,