НАУЧНО-МЕТОДОЛОГИЧЕСКИЕ АСПЕКТЫ В ОБЛАСТИ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

А.Н. Горбач, С.Н. Касанин

В Указе Президента Республики Беларусь от 09.11.2010 № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь» выделены концептуальные источники угроз национальной безопасности в информационной сфере.

В Указе Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации» четко определено в каких целях организуются и проводятся Научно-исследовательские и опытно-конструкторские работы в сфере технической и криптографической защиты информации:

Приказом Государственного комитета по науке и технологиям Республики Беларусь от 30 мая 2016 г. № 93 утверждена государственная научно-техническая программа «Развитие методов и средств системы комплексной защиты информации и специальных технических средств (ГНТП «Защита информации – 3»), на 2016 – 2020 годы.

Эти документы в области технической защиты информации гармонично дополняют и другие соответствующие НПА.

Анализ состояния дел в сфере технической защиты информации показывает:

1. Сложились вполне сформировавшаяся концепция и структура, основу которой составляют:

2. Эффективность и соразмерность мер по защите информации от утечек по техническим каналам в Республике Беларусь позволяет обеспечить защиту информации в соответствии с требованиями действующих нормативно-методических документов и технических нормативных правовых актов.

Исследования в данной области свидетельствуют, что для борьбы с этой тенденцией нельзя ограничиваться отдельными и разовыми мероприятиями, необходим системный подход. Это непрерывный процесс, немаловажное и первостепенное значение в котором отводится развитию и совершенствованию научно-методологических аспектов в области технической защиты информации.

Первое: необходима проработка и конкретизация приоритетных научные исследования в области технической защиты информации.

Второе: значимой для развития исследований в области технической защиты информации остается проблема хронического недофинансирования.

Третье: совершенствование кадровой политики в сфере ТЗИ.

АНАЛИЗ СОСТОЯНИЯ И МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

М.М. Дроздов, А.М. Прудник

В настоящее время идет процесс бурного развития информационных технологий, которые стали неотъемлемой частью нашей жизни. Вместе с этим, возрастает и количество угроз информационной безопасности. По данным МВД Республики Беларусь за прошедший год, количество угроз информационной безопасности в Республике Беларусь увеличилось на 63,6 % [1]. Только количество фактов несанкционированного доступа к компьютерной информации возросло на 152,9 %. В связи с этим, необходима разработка эффективных методов и средств защиты информации. Главной целью, при разработке методов и средств информационной безопасности, является определение критериев защищенности информационных систем, формулировка требований к их уровню защищенности, а также формирование системного подхода к проблеме анализа и синтеза технических и программных средств защиты информации от несанкционированного доступа.

Одним из способов решения данной проблемы является комплексное использование аппаратных и программных средств защиты, которые должны быть ориентированы на комплексное обеспечение эффективного решения функциональных задач информационной системы. Методологически решение этих задач следует осуществлять как проектирование сложной, достаточно автономной программно-аппаратной системы во и взаимодействии с окружающими ее

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,