ПРОГРАММНО-ТЕХНИЧЕСКИЕ АСПЕКТЫ ФУНКЦИОНИРОВАНИЯ СИСТЕМ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Белозеров О.И.[1], Топоркова И.И.[2]

[1]Белозеров Олег Иванович - кандидат технических наук, доцент,
кафедра информационных систем и технологий,
Хабаровский государственный университет экономики и права;
[2]Топоркова Ирина Игоревна - студент,
юридический факультет,
Дальневосточный институт (филиал)
Всероссийский государственный университет юстиции,
г. Хабаровск

Аннотация: *в статье рассматриваются вопросы совершенствования механизмов создания и функционирования систем информационной безопасности. Описаны программно-технические способы и средства обеспечения защиты информационной безопасности от несанкционированного доступа. Обоснована необходимость формирования новых регламентов проведения сертификационных и аттестационных испытаний программно-технического обеспечения.*
Ключевые слова: *информационное общество, информационная безопасность, программно-аппаратные средства.*

Конец XX века характеризуется новым важным этапом научно-технической революции, рождением информационного общества, а также все более значимой ролью информационных технологий в жизни современного общества.

Информационная сфера состоит из информации, субъектов, осуществляющих сбор, формирование, использование и распространение информации, информационной инфраструктуры, системы регулирования возникающих при этом общественных отношений. Она является важнейшим фактором жизни общества и достаточно сильно влияет на состояние экономической, политической, оборонной и других составляющих безопасности Российской Федерации.

В России фундаментом для развития общественных отношений и формирования государственной политики в области обеспечения информационной безопасности, а также главной основой стратегического планирования в этой сфере, является Доктрина информационной безопасности Российской Федерации. [1].

Научно-техническая революция предполагает внедрение во все сферы жизни общества информационно-коммуникационных технологий, формирующих необходимый фундамент для перехода к информационному обществу и оказывающих существенное влияние на многие аспекты жизни личности, общества и государства.

Стратегическим ресурсом становится информация, обладая которым государство и общество уже сегодня могут усилить позиции на международной арене и оказывать влияние на мировые политические, экономические, социальные, культурные и другие процессы, протекающие в международных системах. [4]. И как верно отметила Алиева М.Ф. «информационная безопасность становится важнейшим базовым элементом всей системы безопасности российского государства». [3].

Важнейшей составляющей в комплексной системе защиты является использование программно-аппаратных средств. Данные средства позволяют реализовывать ряд мер, обеспечивающих конфиденциальность информации: идентификацию, аутентификацию, авторизацию, шифрование, контроль целостности, противодействие несанкционированному доступу, противодействие вредоносному программному обеспечению и т.д. Ввиду необходимости в подобных средствах защиты все более актуализируется целесообразность их развития и потребность в разработке новых методов. [2].

К программно-техническим способам и средствам обеспечения защиты информационной безопасности от несанкционированного доступа относятся такие средства защиты, как: средства авторизации, мандатное управление доступом, избирательное управление доступом, управление доступом на основе ролей, журналирование (так же называется Аудит), системы анализа и моделирования информационных потоков (CASE-системы), системы мониторинга сетей, системы обнаружения и предотвращения вторжений (IDS/IPS), системы предотвращения утечек конфиденциальной информации (DLP-системы), анализаторы протоколов, антивирусные средства, межсетевые экраны, криптографические средства, шифрование, цифровая подпись, системы резервного копирования, системы бесперебойного питания, резервирование нагрузки, системы аутентификации, пароль, ключ доступа (физический или электронный), сертификат, биометрия, средства предотвращения взлома корпусов и краж оборудования, средства контроля доступа в помещения, инструментальные средства анализа систем защиты, мониторинговый программный продукт.

Каждое из перечисленных средств может использоваться не только самостоятельно, но и в тесной интеграции с другими. Это делает возможным создание систем информационной защиты любой сложности и конфигурации.

Важной особенностью при использовании программно-аппаратных средств защиты является соответствие международным и российским стандартам, а также их сертификация и лицензирование.

Сертификация на соответствие уровням безопасности проводится Федеральной службой безопасности и ФСТЭК. Федеральная служба по техническому и экспортному контролю осуществляет свои функции в сфере технической защиты информации. Данная служба осуществляет контроль за соблюдением ряда лицензионных требований при осуществлении деятельности по технической защите конфиденциальной информации и по разработке и выпуску средств защиты конфиденциальной информации, в соответствии с действующими национальными оценочными стандартами.

Например, все еще действуют такие национальные оценочные стандарты, как: ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» от 01.01.1996г., «Положение по аттестации объектов информатизации по требованиям безопасности информации» от 25.11.1994г., «Автоматизированные системы (АС). Защита от несанкционированного доступа (НСД) к информации. Классификация АС и требования к защите информации» от 25 июля 1997г., «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» от 04 июня 1999 г. и другие.

Легко заметить, что правовая база, которой руководствуется Федеральная служба по техническому и экспортному контролю, не смотря на год выпуска, до сих пор актуальна и применяется. Она является устаревшей, поскольку в виду научно-технического прогресса появляются качественно новые оборудования, внедряются новые технологии. Например, примером таких новых технологий является облачное хранение данных.

На сегодняшний день, российское законодательство не всегда охватывает все аспекты правового регулирования в сфере обеспечения информационной безопасности, либо, как уже было отмечено, является устаревшим. [5].

Поэтому основной очевидной тенденцией в краткосрочной перспективе должна быть проработка нормативных требований в части технической защиты информации, разработка нормативных документов, регламентирующих порядок построения систем защиты для информационных систем, использующих облачные технологии, а также оценки соответствия таких систем требованиям безопасности информации, формирование новых регламентов проведения сертификационных и аттестационных испытаний программно-технического обеспечения.

Список литературы

1. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СЗ РФ. 2016. № 50. Ст. 7074.
2. Указ Президента РФ от 31.12.2015 № 683 «О Стратегии национальной безопасности Российской Федерации» // СЗ РФ. 2016. № 1. Ст. 212.
3. *Алиева М.Ф.* Информационная безопасность как элемент информационной культуры // Вестник Адыгейского государственного университета. 2012. № 4. С. 63–67.
4. *Бубнов А.В.* Информационная безопасность России в условиях глобализации : автореф. дис. … канд. полит. наук / А.В. Бубнов. М., 2004. 26 с.
5. *Гайдарева И.Н.* Правовое обеспечение информационной безопасности в России // Вестник Адыгейского государственного университета. 2009. № 1. С. 78–85.