УДК 621.396.253

А.А. Смирнов[1], И.А. Лысенко[2]

[1]*Кировоградский национальный технический университет, Кировоград*
[2]*Управление Пенсионного фонда Украины в Кировоградском районе, Кировоград*

АНАЛИЗ СУЩЕСТВУЮЩИХ МЕХАНИЗМОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Представлены основные средства и механизмы информационной безопасности, проведена их классификация. Рассмотрены понятия угрозы и политики безопасности. Исследованы методы криптографической защиты информации, их преимущества и недостатки.

Ключевые слова: *информационная безопасность, угроза безопасности, механизмы информационной безопасности, политика безопасности, криптографические методы защиты.*

Введение

В соответствии с основными положениями Закона Украины "Об информации", Закона Украины "О защите информации в информационно-телекоммуникационных системах", Закона Украины "О государственной тайне", Концепции национальной безопасности Украины [1, 2], первоочередными заданиями в области информатизации и развития связи является построение подсистемы защиты информации.

Необходимость защиты информации, принадлежащей государству, или информации, необходимость защиты которой определена законом, с помощью комплексных систем защиты информации (КСЗИ) определена ст. 8 Закона Украины "О защите информации в информационно-телекоммуникационных системах". Главной особенностью в решении комплекса заданий, которые стоят в этой области, является высокая сложность, обусловленная жесткими вероятностно-временными требованиями, которые предъявляются к форме и способам обработки и передачи информации, к ее своевременности и безопасности [1, 2].

Основная часть

Проведенные исследования [3 – 6] показали, что под информационной безопасностью понимается процесс обеспечивающий конфиденциальность, целостность и доступность информации.

Конфиденциальность информации – определяемая характеристика информации, указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации.

Целостность данных – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Доступность информации – свойство компьютерной системы (среды, средств и технологии обработки), в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ субъектов к интересующей их информации и готовность соответствующих автоматизированных служб к обслуживанию поступающих от субъектов запросов.

В соответствии с тремя основными свойствами безопасности информации различают четыре классические угрозы безопасности, которые представлены на рис. 1.

Для предотвращения угроз безопасности используются соответствующие механизмы информационной безопасности, общая классификация которых представлена на рис. 2. В работах [3, 4] определено что:

– политика безопасности – набор формальных правил, которые регламентируют функционирование механизма информационной безопасности;

– идентификация – определение каждого участника процесса информационного взаимодействия перед тем как к нему будут применены какие было ни было понятия информационной безопасности;

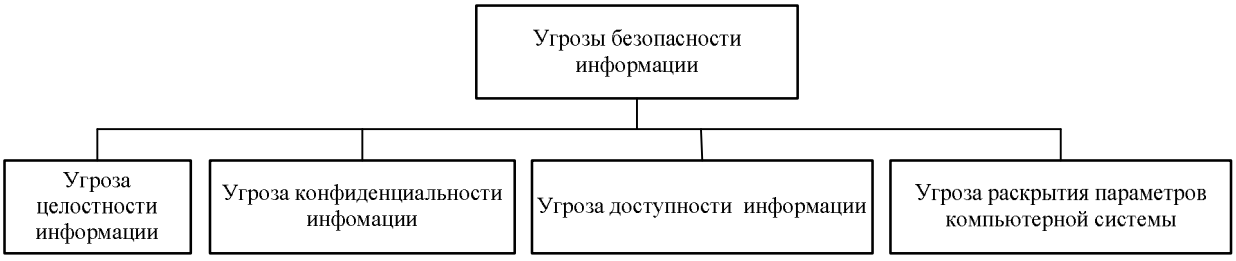

Рис. 1. Общая классификация угроз безопасности информации

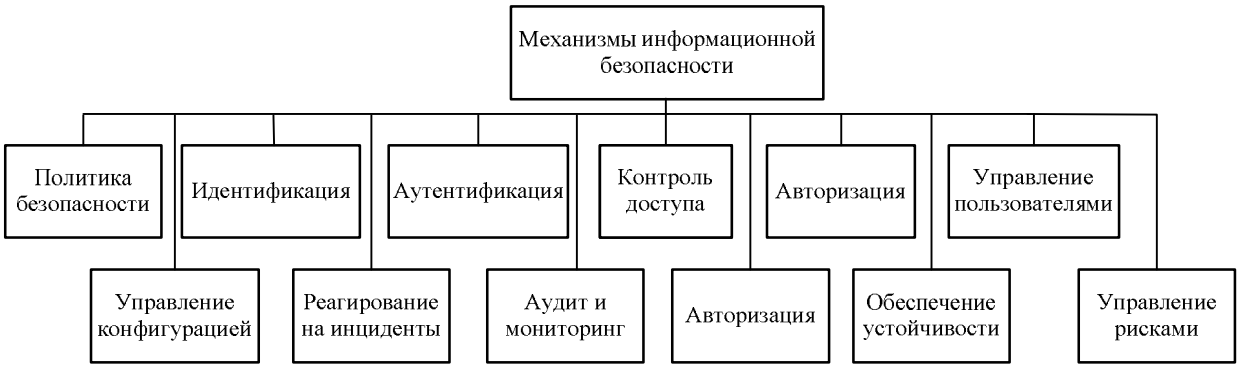

Рис. 2. Общая классификация механизмов безопасности

– аутентификация – обеспечение уверенности в том, что участник процесса обмена информацией идентифицирован верно;

– контроль доступа – создание и поддержание набора правил, определяющих каждому участнику процесса информационного обмена разрешение на доступ к ресурсам и уровень этого доступа;

– авторизация – формирование профиля прав для конкретного участника процесса информационного обмена из набора правил контроля доступа;

– аудит и мониторинг – регулярное отслеживание событий, происходящих в процессе обмена информацией, с регистрацией и анализом предопределенных значимых или подозрительных событий;

– реагирование на инциденты – совокупность процедур или мероприятий, которые производятся при нарушении или подозрении на нарушение информационной безопасности;

– управление конфигурацией – создание и поддержание функционирования среды информационного обмена в соответствии с требованиями информационной безопасности;

– управление пользователями – обеспечение условий работы пользователей в среде информационного обмена в соответствии с требованиями информационной безопасности;

– управление рисками – обеспечение соответствия возможных потерь от нарушения информационной безопасности мощности защитных средств;

– обеспечение устойчивости – поддержание среды информационного обмена в минимально допустимом работоспособном состоянии и соответствии требованиям информационной безопасности в условиях деструктивных внешних или внутренних воздействий.

Исследование общих механизмов безопасности показало, что их использование связано с разработкой политики безопасности, реализацией методик администрирования вычислительных ресурсов, протоколированием событий и аудитом поведения системы безопасности в целом [4].

Основные средства, которые реализуют основные принципы и механизмы информационной безопасности представлены на рис. 3.

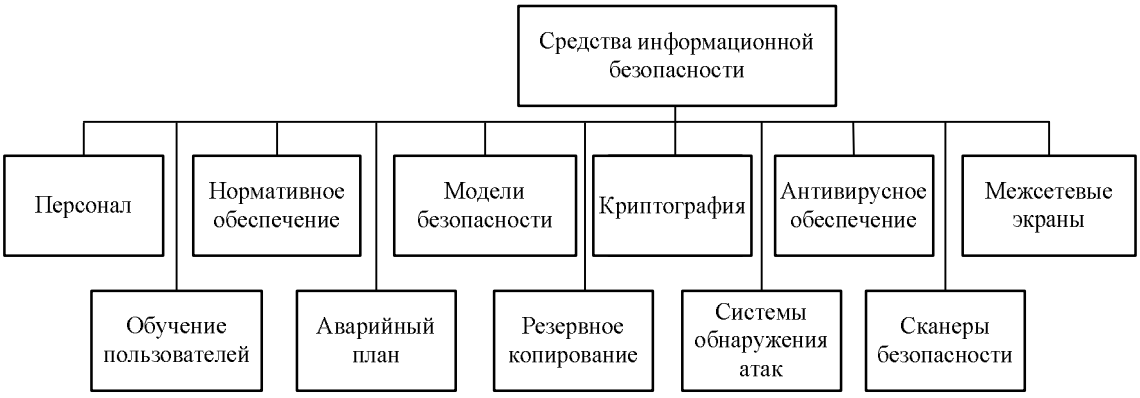

Рис. 3. Средства информационной безопасности

Особое место среди средств информационной безопасности занимает криптография, которая связана с разработкой методов криптографической защиты информации для обеспечения конфиденциальности и аутентичности информации. Исследования [5, 6] показали, что методы криптографической информации делятся на методы симметричной и несимметричной криптографии (рис. 4).

Методы симметричной криптографии основаны на простых и легко реализуемых блоках подстановок и перестановок, что позволяет увеличить скорость шифрования входной информации.

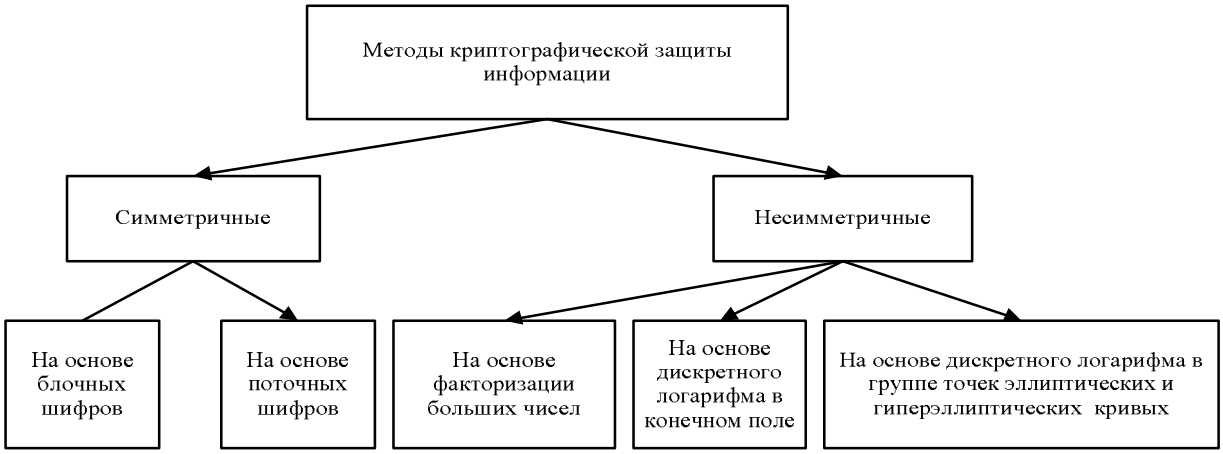

Рис. 4 Криптографические методы защиты информации

Основным недостатком таких систем является использование закрытых каналов связи для передачи ключевых данных, которые используются для шифрования и дешифрования информации.

Методы несимметричной криптографии получили развитие в последние три десятилетия.

Эти методы используют специальные математические методы такие как: факторизация больших чисел, дискретного логарифмирования в группе точек эллиптической и гиперэллиптической кривых.

Несимметричные методы шифрования имеют преимущества и недостатки, обратные тем, которыми обладают симметричные методы [6].

Выводы

Таким образом, проведенный анализ существующих механизмов и средств информационной безопасности показал перспективность развития методов криптографической защиты информации.

При этом комплексное использование симметричных и несимметричных методов позволит в целом повысить эффективность обеспечения услуг безопасности существующими механизмами безопасности.

Список литературы

1. Закон України "Про державну таємницю": Відомості Верховної Ради (ВВР), 1994, N 16, ст. 93. – (Із змінами, внесеними згідно із Законами N 971-IV від 19.06.2003, ВВР, 2003, N 45, ст.361 N 1519-IV від 19.02.2004) [Електрон. ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/3855-12.

2. Закон України "Про Національну систему конфіденційного зв'язку":(Із змінами, внесеними згідно із Законами № 1280-IV від 18.11.2003, ВВР, 2004, № 12, ст.155 N 2599-IV від 31.05.2005) [Електрон. ресурс] – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2919-14.

3. Конеев И.Р. Информационная безопасность предприятия / И.Р. Конеев, А.В. Беляев. – СПб.: БХВ-Петербург, 2003. – 752 с.

4. Галатенко В.А. Информационная безопасность / В.А. Галатенко. – М.: Финансы и статистика, 1997. –158 с.

5. Столингс В. Криптография и защита сетей. Принципы и практика / Вильям Столингс. – М.С-П.К.: Изд. Дом "Вильямс", – 2001. – 670 с.

6. Шаньгин В.Ф. Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: Издательство: ДМК, 2008. – 544 с.

Поступила в редколлегию 20.12.2013

Рецензент: д-р техн. наук, ст. научн. сотр., С.Г. Семенов, Национальный технический университет «ХПИ», Харьков.

АНАЛІЗ ІСНУЮЧІХ МЕХАНІЗМІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

О.А. Смірнов, І.А. Лисенко

Представлені основні засоби та механізми інформаційної безпеки, проведено їх класифікацію. Розглянуто поняття загрози та політики безпеки. Досліджено методи криптографічного захисту інформації, їх переваги та недоліки.

Ключові слова: *інформаційна безпека, загроза безпеки, механізми інформаційної безпеки, політика безпеки, криптографічні методи захисту.*

ANALYSIS OF EXISTING MECHANISMS OF INFORMATION SECURITY

A.A. Smirnov, I.A. Lysenko

The basic tools and mechanisms to provide information security have been presented and classified. The notion of threat and security policy has been scrutinized. The methods of cryptographic protection of information, their advantages and disadvantages have been explored as well.

Keywords: *information security, security threat, the mechanisms of information security, security policy, protection of cryptographic methods.*