ПРЕИМУЩЕСТВА ПРИМЕНЕНИЯ ПРОГРАММНО-ТЕХНИЧЕСКИХ СРЕДСТВ УПРАВЛЕНИЯ ЗАЩИТОЙ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СЕТЯХ

Государственное учреждение
«Научно-исследовательский институт Вооруженных Сил Республики Беларусь»
г. Минск, Республика Беларусь

Мацылевич А. Р.

Утин Л.Л. – к-т. техн. наук, доцент

Субъективные факторы являются одними из наиболее опасных факторов, влияющих на защиту информации, особенно в системах управления процессами обеспечения информационной безопасности. Максимально возможное исключение человека из контура управления защитой информации требует определения обоснованных путей его реализации, одним из которых является разработка и применение в информационных сетях программно-технических средств управления защитой информации.

Используемые в настоящее время информационные сети для обеспечения деятельности органов государственного управления, субъектов экономики государства являются сложными организационно-техническими системами. С одной стороны, внедрение цифровых информационных технологий обеспечивает повышение эффективности управления подчиненными силами и средствами, с другой стороны, их использование привело к появлению принципиально новых угроз защищенности информации, ущерб от воздействия которых может снизить эффективность управления, вплоть до его срыва. Решение этого противоречия в процессе информатизации общества является и будет являться наиболее актуальным.

Рис. 1 – Структурная схема выявленного противоречия в защите информации

Вышеуказанные угрозы имеют техногенную природу, вследствие чего, человек, в силу своих психофизиологических возможностей, не в состоянии своевременно и адекватно на них реагировать (противодействовать).

В целях защиты информации в информационных сетях применяются разноплановые технические средства защиты информации, непосредственное управление которыми человеком не обеспечивает оперативность реагирования на возникающие угрозы защищенности информации. Это вызвано необходимостью использования ресурсоемких интерфейсов. Кроме того, эффективность выявления угроз защищенности информации и выработки рациональных способов их нейтрализации находится в зависимости от таких свойств человека как мотивация, профессиональная подготовленность, усталость, отвлеченность, эмоциональность и других, что в некоторых случаях может привести к блокированию работы системы защиты информации в информационной сети.

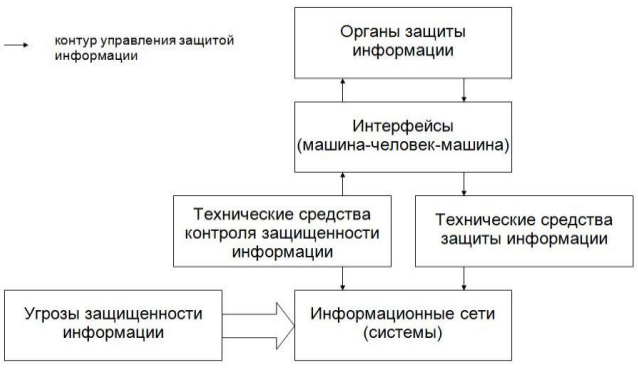

Рис. 2 – Структурная схема существующей системы управления защитой информации

Максимально возможное исключение антропогенного фактора из процессов управления защитой информации возможно путем передачи части функций управления защитой информации на программно-технический уровень, посредством применения программно-технических средств, реализующих функции управления защитой информации. Это позволит наиболее эффективно решать задачи единого управления защиты информационных ресурсов, распределенных в информационных сетях. При этом максимально исключив из контура управления защитой информации «человеческий фактор». В перспективе такие средства целесообразно интегрировать в существующие системы защиты информации информационных сетей.

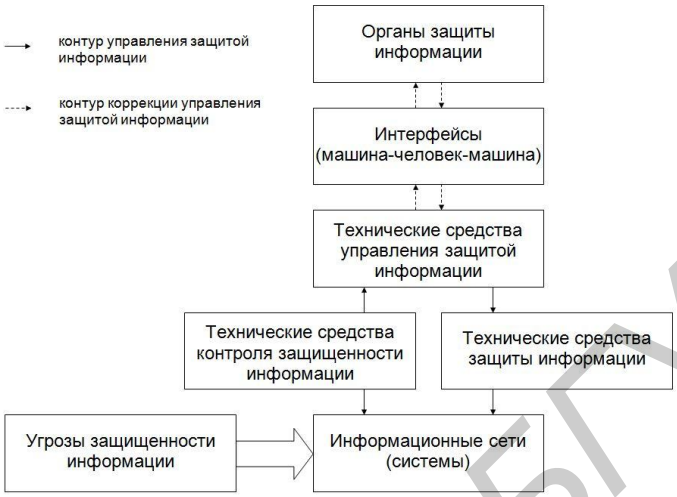

Рис. 3 – Предлагаемый подход к разрешению выявленных противоречий

Определение наиболее эффективных способов применения программно-технических средств, реализующих функции управления защитой информации в информационных сетях, является актуальным.

Достигнуть этого предлагается путем решения ряда научных задач:

разработать методику управления защитой информации в информационных сетях посредством применения программно-технических средств;

определить способы применения программно-технических средств управления защитой информации в информационных сетях;

оценить эффективность способов применения программно-технических средств управления защитой информации в информационной сети;

разработать рекомендации по созданию и применению программно-технических средств управления защитой информации в информационных сетях.

Список использованных источников:

1. Об информации, информатизации и защите информации, Закон Респ. Беларусь от 10.11.2008 № 455-З, текст по состоянию на 1.03.2015. – Минск – 21 с.
2. Защита информации Основные термины и определения, СТБ ГОСТ Р 50922-2000: - Введ. 22.05.2000 – Минск: Государственное проектное и научно-исследовательское предприятие «Гипросвязь», 2000. – 6 с.