Сфера информационной безопасности в настоящее время претерпевает значительные изменения, связанные с практически повсеместным действием ряда глобальных вызовов. К числу таких вызовов в первую очередь можно отнести пандемию и активизацию процессов цифровизации. Последняя в силу значительного влияния на информационную сферу требует адекватного изменения в структуре систем защиты информации, которые бы обеспечили эффективное противодействие новым угрозам. Пандемия, помимо ускорения процесса внедрения цифровых решений, продуктов и сервисов, вызвала и еще целый ряд эффектов и явлений, которые требуют ответа со стороны систем информационной безопасности организаций. Работа в дистанционном и смешанном режимах, перенос заметной части бизнес-процессов в виртуальное пространство обусловили высокую подвижность границ информационного периметра. Многие организации, несмотря на соблюдение всех прежних требований к информационной безопасности, имея уже сформированную и действующую систему, имеющую комплексный характер и все необходимые атрибуты хорошей защиты информации, оказались, тем не менее, не готовыми к такой подвижности границ. Тем самым, значительно возросла роль «эластичности» систем информационной безопасности, их способности быстро перестраиваться и адаптироваться к изменению информационного периметра организации.

Целью данной работы является развитие и теоретическое обоснование мероприятий и решений по обеспечению информационной безопасности организации при изменении периметра защиты.

В соответствии с поставленной целью сформулированы задачи:

1. Исследовать особенности создания информационного периметра в условиях действия ряда современных вызовов.

2. Рассмотреть наиболее распространенные виды киберугроз, факторы и причины их возникновения и распространения.

3. Рассмотреть возможные способы построения эффективных систем информационной безопасности в условиях пандемии и постпандемии.

4. Провести сравнительный анализ средств мониторинга по различным параметрам. Разработать рекомендации по выбору и настройке средств мониторинга.

5. Предложить мероприятия по улучшению эластичности систем информационной безопасности организации.

Подробно рассмотрены принципы их работы, описаны положительные стороны и недостатки, показана важность их использования для обеспечения полноценной защиты. В работе обоснованы наиболее популярные бесплатные и платные инструменты мониторинга, приведены особенности каждого программного продукта. Рассмотрены разработки как зарубежных, так и отечественных компаний, а также проведен сравнительный анализ этих средств по различным параметрам. В завершении описан набор рекомендаций для системных администраторов по выбору и применению средств мониторинга сетевых объектов, который позволит обеспечить высокий уровень защищенности информационного периметра.