УДК 004.75

Концептуальная модель централизованного управления комплексом программно-аппаратных средств защиты информации в сети как средство повышения вероятности обнаружения нарушений

Клевцов И. А. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Научный руководитель – к.т.н., доцент Коржук В. М. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»)

Введение. В данной работе была рассмотрена концепция централизованного управления средствами защиты информации, составляющих контур информационной безопасности. Также представлена концептуальная модель с описанными процессами взаимодействия центра управления с программно-аппаратным комплексом средств защиты информации на базе полученных сведений от программного алгоритма оценки динамических характеристик (поведение пользователя за компьютером, работа с документами, использование VPN) с целью оптимального применения средств защиты информации, а также повышения вероятности обнаружения нарушений.
Взаимодействие центра управления с программно-аппаратным комплексом средств защиты включает в себя возможность выбора, итерации и одновременное выполнение подготовленных алгоритмов и политик, а также оповещения администратора об инцидентах информационной безопасности.
Основной идеей концепции централизованного управления средствами защиты информации является возможность интеграции данной модели в организации, работающих на базе технологий Индустрии 4.0.

Основная часть. В большинстве организаций имеются ограничения по затрачиваемым ресурсам на обеспечение информационной безопасности. А также не всегда имеется возможность централизованно управлять программно-аппаратным комплексом средств защиты информации, что является одним из ключевых факторов на оперативность обработки инцидента информационной безопасности и применение мер по устранению.
Программный алгоритм оценки динамических характеристик совместно с центральным управлением средствами защиты информации позволит оптимально распределять ресурсы средств защиты информации.

Заключение. В ходе проделанной работы была предложена концептуальная модель централизованного управления комплексом программно-аппаратных средств защиты информации. Приведен алгоритм оценки динамических характеристик, для распределения ресурсов средств защиты информации, рассматриваемой базой для которого служит профиль поведения пользователя за персональным компьютером, обрабатываемая им информация, используемое программное обеспечение для обхода ограничений политик информационной безопасности, а также наличие прав администратора.
Для дальнейшего исследования необходимо определить возможные наборы программно-аппаратных и технических средств защиты информации, расширить перечень

операционных систем для базирования центра управления, чтобы увеличить применимость модели.

Клевцов И. А. (автор)

Коржук В. М. (научный руководитель)