О НЕОБХОДИМОСТИ РАЗВИТИЯ КОНЕПЦИИ ПРОАКТИВНОЙ ЗАЩИТЫ

Осипов П.А.[a], Минзов А.С.[b]

Государственное бюджетное образовательное учреждение высшего образования
Московской области «Университет «Дубна»;
Россия, 141980, Московская область, г. Дубна, ул. Университетская, д. 19, к. 1-312;
[a]89154201230, osipov.pavel92@gmail.com;
[b]89265650570, 926-565-0570@mail.ru

Развитие корпоративных информационных систем (КИС) сегодня является важным условием повышения эффективности бизнес-процессов за счет использования ресурсов глобальных информационных систем, но с другой стороны увеличивает вероятность реализации угроз к ним со стороны внешней среды через портальные решения. Однако, существующие системы защиты КИС не могут обеспечить полноценной защиты, что можно увидеть из статистики компании «Лаборатории Касперского» за 1 квартал 2017 года, а также по последним событиями с вирусами-шифровальщиками WannaCry, Petya, BadRabbit [1].

В этих условиях наиболее перспективными являются методы обнаружения признаков начала атак и прогнозирования развития сценариев инцидентов. Такие методы относятся к механизмам проактивной защиты.

На сегодняшний день, внимание к проактивным методам защиты информации со стороны производителей программного обеспечения явно недостаточно. Это во многом объясняется отсутствием теории проактивной защиты информации и механизмов её реализации. Наиболее распространенный класс проактивных систем защиты относится к DLP-системам. Однако он ориентирован только на предотвращение утечек информации КИС во внешнюю среду, что явно недостаточно. Другие решения на основе механизмов проактивной защиты в антивирусных программах не способны обеспечить надежное выявление начала атак, поэтому зачастую такие решения идут, как дополнительный функциональный модуль.

Все это приводит к необходимости разработки концепции проактивной защиты, которая способна обеспечивать защиту информационных систем от большинства новых угроз без применения сигнатурных методов. Проактивные системы информационной безопасности должны учитывать функциональность и архитектуру защищаемой информационной системы, а также обеспечивать эффективный мониторинг поведения критических элементов информационных систем. Они должны обеспечивать защиту от новых видов угроз, но при этом стоимость внедрения подобного рода систем должна быть значительно ниже, чем стоимость защищаемых активов.

Целью работы является создание концепции проактивной системы защиты информации, которая позволит обеспечить полностью защиту КИС на основе применения методов искусственного интеллекта.

Литература

1. *Роман Унучек, Федор Синицын, Денис Паринов, Владислав Столяров.* Развитие информационных угроз в первом квартале 2017 года. Статистика. URL:https://securelist.ru/it-threat-evolution-q1-2017-statistics/30657/, 2017.