УДК 004.056.2

Разработка метода корреляции событий информационной безопасности в сетевом трафике

А.Д. Бартов, Федеральное государственное автономное образовательное учреждение высшего образования „Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики“, Санкт-Петербург

Научный руководитель – к.т.н., доцент А. И. Спивак, Федеральное государственное автономное образовательное учреждение высшего образования „Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики“, Санкт-Петербург

Введение.

Существует множество вариантов получения нарушителем ценной для компании информации: применение методов социальной инженерии, утечка информации, несанкционированный доступ. Так же происходят атаки и по каналам связи, таким как интернет.

Когда происходит инцидент, нарушающий информационную безопасность компании, то эта компания зачастую терпит убытки. Последствия от получения прав на действия с данными бывают разными, например, уничтожение, шифрования с требованием выкупа и передача конкурентам. Все эти события можно было предотвратить, если система обнаружения вторжений могла предсказывать и выявлять атаки. Перед ее осуществлением злоумышленники сначала подготавливают сценарий нападения и изучают инфраструктуру предприятия и только потом осуществляют задуманное.

Для решения данной задачи был выбран метод корреляции событий в сетевом трафике. Данное решение позволяет узнать коэффициент того, что будет произведена атака на основе событий происходящих на предприятии. Иными словами у ответственного лица за информационную безопасность объекта будет информация следующего характера, какие действия происходят и на что они направлены в рамках фазы подготовки к нарушению защиты предприятия.

Цель.

Разработать метод корреляции событий информационной безопасности в сетевом трафике.

Базовые положения исследования.

Для реализации данного метода необходимо рассмотреть потенциальные модели угроз, используя которые мы можем написать корреляционную функцию и создать модель события информационной безопасности и описать метод.

В момент его описания необходимо учитывать и тот фактор, что нужно поддерживать, обновлять (усовершенствовать) и дополнять модель. Данную процедуру необходимо осуществлять с целью поддержание актуальности и работоспособности системы. В противном случае, в мире в котором нарушение информационной безопасности осуществляются с большой частотой и с большой скоростью появляются новые виды атак и подходы к вторжению путем использования сети интернет компании, затрагивающие данные компании.

Важной составляющей в определении входных значений является выбор характеристик событий сетевого трафика. Это осуществляется путем детального изучения подготовительной фазы «взлома», тем самым мы будем понимать, какие характеристики стоит рассматривать для корреляционного анализа.

Промежуточные результаты.

В работе описываются процессы сбора необходимой для построения модели информации, которую будем использовать для корреляции, определения необходимых и возможных параметров модели и построения непосредственно самой модели. Собраны и проанализированы подготовительные этапы и атаки с целью выявления характеристик для входных данных, которые будем использовать в методе а так же рассмотрели, что должно быть в виде выходного параметра.

Основной результат.

В ходе работы были предложены методы применения корреляционного анализа к сетевому трафику для выявления и предсказания атак. В дальнейшем нужно будет либо выбрать один из них, либо использовать комплексное применение данного решения.

Авторы:	«__»_____2019	_____	А.Д. Бартов
Научный руководитель:	«__»_____2019	_____	А.И. Спивак
Декан факультета БИТ:	«__»_____2019	_____	Д.А. Заколдаев