УДК 004.492.2

ПРОГНОЗИРОВАНИЕ ПОТЕРЬ, СВЯЗАННЫХ С РЕАЛИЗАЦИЕЙ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Хамидуллина Е.Д.[1)], Губенко Н.Е. [2)]
Донецкий национальный технический университет
[1)] магистрант; [2)] к.т.н., доцент

I. Постановка проблемы

Любая предпринимательская деятельность сопряжена с получением, хранением и обработкой какой-либо информации. Далеко не каждый предприниматель готов вести честную конкурентную борьбу, поэтому в последнее время потери от реализации угроз информационной безопасности могут привести к серьезным проблемам в сфере ведения бизнеса.

Безусловно, основной задачей отдела информационной безопасности (ИБ) является защита основных свойств информации (доступность, целостность, конфиденциальность). Однако не маловажным остается тот факт, что реализовать угрозы было бы намного сложнее, если бы предприниматель заранее знал о возможности существования такой угрозы и о возможных потерях, к которым может привести ее реализация. Поэтому прогнозирование потерь от угроз ИБ становится важным аспектом при составлении бизнес-плана.

II. Цель работы

Целью данного исследования является определение наиболее часто встречаемых угроз, а также поиск новых методов прогнозирования угроз ИБ.

III. Угрозы ИБ, которые чаще всего встречаются в современном мире

Существует огромное количество угроз, реализация которых может привести предприятие к потерям. Ниже представлен список наиболее распространенных из них [1]:

- вредоносные программы;
- злонамеренные сотрудники;
- использование уязвимостей;
- невнимательные работники;
- мобильные устройства;
- социальные сети;
- социальная инженерия;
- атаки нулевого дня;
- угроза безопасности облачных вычислений;
- кибер-шпионаж.

Так, компания Sophos отмечает значительный рост вредоносных программ, а также спама и фишинга (виды социальной инженерии) за 2009-2010 год (рис. 1). Также исследования этой компании показывают, что 34% всех вирусов на момент 2011 года было создано в 2010 году [2].

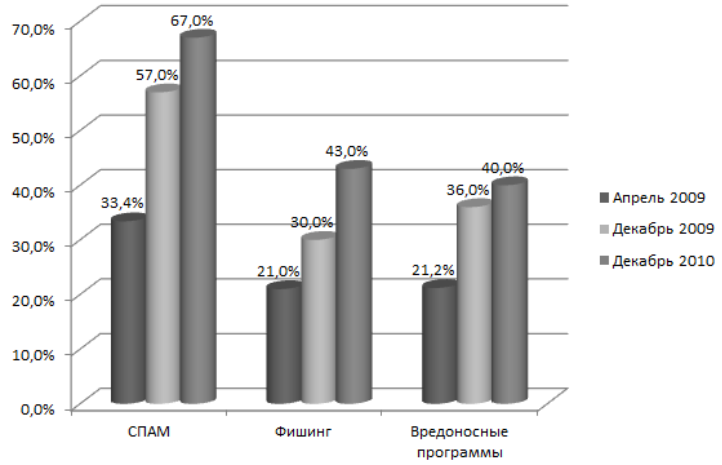

Рисунок 1 – Сравнительная характеристика количества угроз за 2009-2010 гг.

IV. Прогнозирование угроз информационной безопасности

В последнее время теория ритмов приобрела большую значимость в области прогнозирования потерь, связанных с реализацией угроз информационной безопасности. Суть этой теории состоит в том, что все процессы природного, экономического, технологического и других характеров подчиняются определенным общим закономерностям. На основе этой теории Научным обществом студентов создан продукт «Future», в рамках которой, среди прочих проблем, есть возможность решить также некоторые проблемы прогнозирования информационных угроз [3].

Однако статистические методы все еще являются важными для прогнозирования. Главным преимуществом этих методов является адаптация математических и статистических аппаратов к объекту. Статистические методы универсальны, поскольку для проведения анализа не требуется знания о возможных атаках и используемых ими уязвимостях. Но при использовании этих методик возникает ряд проблем:

«статистические» системы не чувствительны к порядку следования событий;

трудно задать граничные (пороговые) значения отслеживаемых системой обнаружения атак характеристик;

«статистические» системы могут быть с течением времени «обучены» нарушителями.

Еще один метод прогнозирования, использующийся в работе – метод экспертных оценок. Он основывается на использовании знаний экспертов в данной области, формулируемых в базе данных, пример которой приведен на рисунке 2, с большинством известных в современном мире угроз. База данных поможет в поиске аналогичных происшествий и методов их решения, а также минимизации потерь. Такой метод прогнозирования имеет много общего с прогнозированием методом аналогий. Главным достоинством такого прогнозирования является отсутствие ложных тревог.

Основным недостатком является невозможность отражения неизвестных атак. При этом даже небольшое изменение уже известной атаки может стать серьезной проблемой [4].

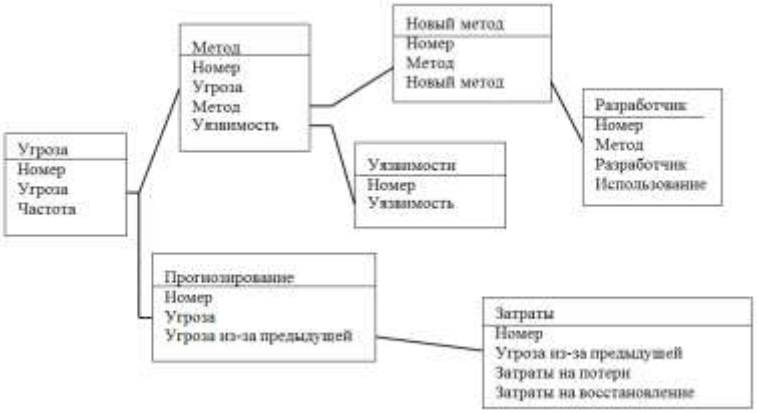

Рисунок 2 – Схема базы данных

Вывод

Появление Интернет и информационных систем позволило предприятиям снизить затраты, добиться большего охвата рынка и т.д.

Важно понимать, что каждый бизнес должен быть защищен. Поэтому важно осознавать все проблемы, которые могут возникнуть. В данной статье приведены основные угрозы, которые могут возникнуть в информационной сфере предприятия.

Важно также отметить, что уровень безопасности может быть улучшен с помощью прогнозирования будущих угроз. Данная сфера информационной безопасности еще требует улучшений и доработок, для того, чтобы обеспечить наибольшую конкурентоспособность предприятий, а также ведение честного бизнеса.

Список использованных источников

1. Топ-10 угроз информационной безопасности/ Интернет-ресурс. - Режим доступа: www/ URL:http://www.net-security.org/secworld.php?id=8709.
2. 2011 г. Обзор по материалам ведущих фирм мира, работающих в сфере сетевой безопасности/ Интернет-ресурс. - Режим доступа: www/ URL: http://book.itep.ru/10/2011.htm#43.
3. Бузинов А.С., Жигулин Г.П., Шабаев Р.И. Моделирование и прогнозирование информационных угроз как составная часть Концепции информационной безопасности РФ – СПб: Издательство «Научно-производственное объединение специальных материалов», - 2010. – С.63-68.
4. Технологии обнаружения атак/ Интернет-ресурс. - Режим доступа: www/ URL: http://ypn.ru/448/intrusion-detection-technologies/