УДК 004.492.2

Е.Д. Хамидуллина, Н.Е. Губенко
Донецкий национальный технический университет, г. Донецк
кафедра компьютерных наук и технологий

ПРИМЕНЕНИЕ ПРОГНОЗИРОВАНИЯ МЕТОДОМ АНАЛОГИЙ К ОЦЕНКЕ ПОТЕРЬ, СВЯЗАННЫХ С УГРОЗАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация

Хамидуллина Е.Д., Губенко Н.Е. Применение прогнозирования методом аналогий к оценке потерь, связанных с угрозами информационной безопасности. *Главной целью данной статьи является рассмотрение основных принципов информационной безопасности. Рассмотрены методы анализов рисков, а также модель оценки, связанных с угрозами информационной безопасности. Предложен метод аналогий для прогнозирования реализаций угроз. Модель может быть использована для компаний, которые нуждаются в защите, а также для подсчета потерь в случае необходимости.*

Ключевые слова: *информационная безопасность, угроза, анализ рисков, модель, потери.*

Постановка проблемы. В настоящее время, вопрос информационной безопасности является неотъемлемой частью управления бизнесом.

Несмотря на то, что термины информационная безопасность, компьютерная безопасность и обеспечение информационной безопасности взаимосвязаны и имеют общие цели защиты конфиденциальности, целостности и доступности информации, между ними есть некоторые различия.

Информационная безопасность зависит от формы представления данных: электронная, печатная или другие формы. Компьютерная безопасность обеспечивает наличие и правильность работы компьютерной системы. Она не может работать с информацией, которая хранится и обрабатывается с помощью компьютера. Обеспечение безопасности информации сосредотачивается на причинах обеспечения защиты для информации.

Область информационной безопасности значительно выросла и развилась в последние годы. Это очень существенная часть безопасности и компьютерных исследований [1].

Цель статьи – провести анализ оценки потерь, связанных с угрозами информационной безопасности, а так же предложить прогнозирование методом аналогий в качестве совершенствования системы информационной безопасности.

Топ-10 угроз информационной безопасности. Существует огромное количество угроз, которые могут привести любую компанию к большим потерям. Список наиболее распространенных из них представлен ниже [2]:

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

Существует еще один вариант классификации угроз информационной безопасности (рис. 1) представленный компанией Verizon [3].

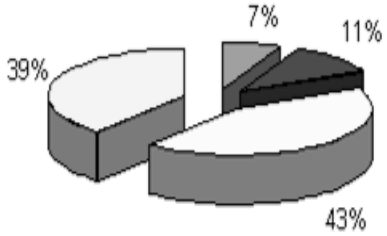

Рисунок 1 – Классификация угроз информационной безопасности

В соответствии с ней на первом месте только внешние угрозы (43%),
на втором месте – множественные угрозы (39%),
на третьем месте - угрозы, вызванные внутренними уязвимостями (11%) и
на четвертом месте – угрозы со стороны инсайдеров и партнеров (7%).

Количественный анализ рисков. Этот метод анализа риска использует два основных элемента: вероятность события и вероятные потери в случае возникновения этого события.

Годовые ожидаемые убытки (ALE) рассчитываются путем простого умножения потенциальных потерь на вероятность.

Таким образом, теоретически можно оценить степень риска событий (ALE) и принимать решения, основываясь на этом.

С другой стороны, ненадежность и неточность данных делают этот метод сложным для использования. Кроме того, элементы управления и контрмеры часто работают с рядом потенциальных событий и сами события часто взаимосвязаны.

Качественный анализ рисков. В отличие от предыдущего анализа качественный метод не требует вероятности события и возможных потерь в случае его возникновения. Вместо этого он использует целый ряд взаимосвязанных элементов:

– Угрозы (то, что может атаковать систему);

– Уязвимости ("ахиллесова пята" системы, например, для пожарной безопасности уязвимость состоит в присутствии легковоспламеняющихся материалов.);

– Управление (контрмеры),

и четыре типа контроля [4]:

– Сдерживающий фактор управления уменьшает вероятность преднамеренного нападения;

– профилактический контроль делает нападение неудачным или уменьшает его последствия;

– корректирующее управление уменьшают эффект от нападения;

– детективный контроль обнаруживает атаки и вызывает профилактический или корректирующий контроли.

Эти элементы можно проиллюстрировать на простой реляционной модели (рис. 2).

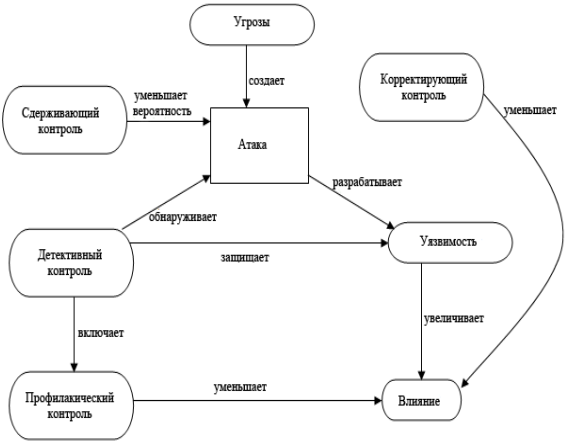

Рисунок 2 – Реляционная модель элементов качественного анализа рисков

Анализ модели оценки потерь. Целью каждого предприятия является максимизация прибыли и минимизация затрат. Если первая задача зависит от руководства, то вторая в определенной степени зависит от отдела информационной безопасности (ИБ), т.к. отдел ИБ работает с проблемами защиты главных свойств информации (доступности, целостности, конфиденциальности).

Угроза доступности – это ограниченность доступа к ресурсу или полное его отсутствие. Ресурс исчерпан при наличии доступа к ресурсу с затратой большого промежутка времени.

Потери от угроз доступности рассчитываются по формуле:

$$L = L_{ul} + L_r + L_d + L_{li},$$

где L_{ul} – потери от несвоевременного оказания услуг по доступу к информации; L_r – потери, связанные с восстановлением работоспособности; L_d – потери, связанные с простоем узла системы (УС); L_{li} – потери, связанные с потерей дохода.

Формула для расчёта потерь, связанных с восстановлением работоспособности:

$$L_r = \frac{\sum_{i=1}^{n} S_i}{T} * t_r,$$

где S_i — зарплата в месяц сотрудника, восстанавливающего работоспособность атакованного узла системы (АУС); N — количество сотрудников, восстанавливающих работоспособность АУС; t_r — время восстановления работоспособности; T — количество рабочих часов узла системы в месяц.

Потери, связанные с простоем АУС рассчитываются по формуле:

$$L_d = \frac{\sum_{i=1}^{n} S_i}{T} * t_d,$$

где S_i — зарплата в месяц сотрудника АУС; N — количество сотрудников АУС; t_d — время простоя АУС; T — количество рабочих часов узла системы в месяц.

При этом важно понимать, что во время реализации угрозы доступности происходит потеря дохода, которая рассчитывается по формуле:

$$L_{li} = Inc * \frac{t_r + t_d}{T} \ ,$$

где Inc – годовой доход от использования АУС; t_r — время восстановления АУС; t_d — время простоя АУС; T — период работы системы в течение года.

Целостность данных означает их полноту и неизменность. Угроза целостности представляет собой реализацию изменения данных преднамеренно или непреднамеренно. Формула расчета потерь, связанных с угрозами целостности:

$$L = L_{um} + L_r + L_d + L_{li},$$

где L_{um} — потери от несанкционированной модификации информации, размер потерь будет зависеть от значимости информации, целостность которой нарушена; L_r — потери, связанные с восстановлением работоспособности; L_d — потери, связанные с простоем узла системы; L_{li} — потери, связанные с утратой возможного дохода.

Потери, связанные с восстановлением работоспособности рассчитываются по формуле:

$$L = L_{ri} + L_{rc},$$

где L_{ri} — потери, связанные с восстановлением информации; L_{rc} — потери, связанные с заменой поврежденных компонент, являются фиксированными материальными затратами.

Восстановление информации так же связанно с потерями, которые рассчитываются по формуле:

$$L_{ri} = \frac{\sum_{i=1}^{n} S_i}{T} * t_{ri},$$

где S_i — зарплата в месяц сотрудника атакованного узла системы; N — количество сотрудников на атакованном узле системы; t_{ri} — время, необходимое для восстановления информации на атакованном узле системы; T — количество рабочих часов узла системы в месяц.

При этом во время реализации угрозы предприятие не получает доход. Поэтому потери, связанные с утратой возможного дохода, определяются по формуле:

$$L_{li} = Inc * \frac{t_r + t_d + t_{ri}}{T} \ ,$$

где Inc — годовой доход АУС; t_d — время простоя АУС; t_r — время восстановления АУС; t_{ri} — время восстановления информации на атакованном АУС; T — период работы системы в течение года.

Конфиденциальная информации — информация, не являющаяся общедоступной и могущая нанести ущерб правам и охраняемым законом интересам предоставившего ее лица. Потери при разлашении информации могут быть финансовыми, потерей репутации и конкурентоспособности.

Поэтому для расчета потерь наиболее удобным является метод экспертных оценок. Сущность метода заключается в том, что группа специалистов в данной области и анализируют потери, исходя из значимости самой информации.

Из вышесказанного понятно, что информацию на преприятии необходимо защищать с целью минимизации потерь. Для этого используют страхование информационных рисков предприятия (выдача страховыми обществами гарантий субъектам информационных отношений по восполнению материального ущерба в случае реализации угроз информационной безопасности).

С использованием страхования информационных рисков предприятия итоговые потери (L*) рассчитываются по формуле

$$L^* = L - Ins,$$

где L — суммарные потери из-за нарушения нескольких категорий информации; Ins — суммарная прибыль от страхования рисков.

Прогнозирование потерь. Прогнозирование является важной частью любого бизнеса. Важно понимать, что довольно трудно обнаружить угрозы, прежде чем они появятся. Чтобы быть готовым к этому важно также быть всегда в курсе последних новостей связанных с технологиями и использовать прогнозирование методом аналогий. Прогноз методом аналогий предполагает, что два или несколько явлений имеют одни и те же модели поведения [5].

Это означает, что ИТ-менеджеры могут изучать подобную ситуацию, которая произошла до или с другой компанией и попытаться предсказать угрозу

Для того чтобы следить за частотой угроз и методами, которые были использованы ИТ-менеджерами, чтобы избежать проблем или для улучшения системы должна быть разработана база данных с необходимой информацией компании.

Пример такой базы данных показан на рисунке 3.

Важно помнить, все методы, которые были использованы, чтобы избежать угроз и обнаружить уязвимости этих методов. Поэтому таблица "Методы" является важной частью данной базы.

Добросовестные менеджеры всегда стараются найти новые методы борьбы с угрозами. Они могут быть отражены в таблице, "Новый метод".

Прогноз методом аналогий означает, что менеджер должен обнаружить похожую информацию о прошлом. Итак, таблица "Прогнозирование" может помочь оценить ситуацию и сравнить ее с такой же в прошлом.

Таблица "Разработчик" может помочь узнать информацию о разработчиках методики борьбы с угрозами и где эти методики могут быть использован.

Для того чтобы предсказать будущие убытки ИТ-менеджеры должны знать, какие расходы понесла компания в такой же ситуации в прошлом. Они также должны принять во внимание инфляцию.

Развитие базы данных является важной частью прогнозирования методом аналогий. Намного легче проследить за угрозами и последствиями при наличии хорошо структурированной базы данных.

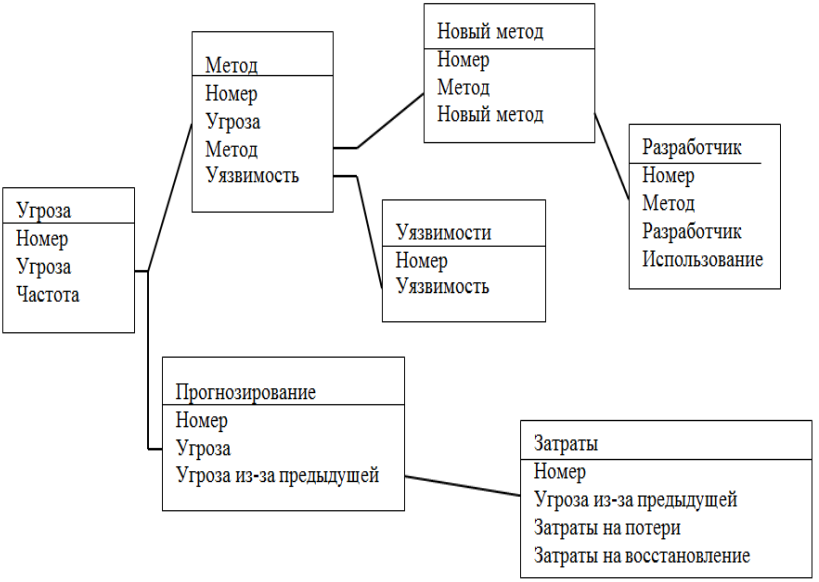

Рисунок 3 – Схема базы данных

Выводы. 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 этой статье указаны топ-10 угроз, которые составляют наибольшую проблему для бизнеса.

Кроме того, существует возможность оценить потери, которые вызваны угрозами. Есть несколько подходов, которые могут помочь оценить потери от нескольких видов рисков.

Важно также отметить, что уровень безопасности может быть улучшен с помощью прогнозирования будущих угроз. Очень важно использовать несколько видов прогнозирования для того, чтобы получить лучшую модель. Это может помочь менеджерам избежать больших потерь.

Таким образом, можно сделать вывод, что важность анализа рисков является неоспоримой.

Список литературы

1. Информационная безопасность/ Интернет-ресурс. – Режим доступа: www/ URL: http://en.wikipedia.org/wiki/Information_security.

2. Топ-10 угроз информационной безопасности/ Интернет-ресурс. - Режим доступа: www/ URL:http://www.net-security.org/
secworld.php?id=8709.

3. 2009 Data Breach Investigations Report / Интернет-ресурс. - Режим доступа: www/ URL: http://www.verizonenterprise.com/resources/
security/reports/2009_databreach_rp.pdf?__ct_return=1.

4. The security risk analysis directory / Интернет-ресурс. - Режим доступа: www/ URL: http://www.security-risk-analysis.com/introduction.htm.

5. McAfee report. Threat prediction / Интернет-ресурс. - Режим доступа: www/ URL: http://www.mcafee.com/us/

6. B.D. Jenkins Security Risk Analysis and Management – Countermeasures Inc., 1998.

7. Zeki Yazar A qualitative risk analysis and management tool – CRAMM – SANS Institute InfoSec Reading Room.

8. Грездов Г.Г. Способ решения задачи формирования комплексной системы защиты информации для автоматизированных систем 1 и 2 класса [Текст] – Киев : ЧП Нестреровой, 2005. – С.66.