ЭКОНОМИЧЕСКИЕ НАУКИ

АНАЛИЗ МЕТОДОВ ОЦЕНКИ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ПРЕДПРИЯТИИ

САХНО Виталий Викторович
магистрант
ФГБОУ ВО «Донской государственный технический университет»
г. Ростов-на-Дону, Россия

В настоящее время, под возможностью атак злоумышленников находиться практически каждая компании. Защита информации играет важная роль, от нее уровня зависит, потеряет ли данных компания, или выйдет из строя телекоммуникационного оборудования, что грозит большими убытками для компании.

Ключевые слова: угрозы, информационная безопасности, оценка рисков, средства защиты.

В настоящее время информационная безопасность становится все больше и больше значимым аспектом при проектировании системы защиты предприятия. Система защиты информации составляет определенную деятельность по предотвращению утечки и распространения информации, несанкционированного доступа к потоком информационных ресурсов предприятия и других негативных воздействий на систему [5]. В данном случаи, именно своевременная и точная оценка рисков угроз информационной безопасности снижает или даже полностью устраняет угрозы, поэтому это является актуальной проблемой на предприятии.

Выделяют три основных источника угроз информационной безопасности [2]:

– техногенные;

– природные;

– человеческие, данные угрозы разделяют на две: преднамеренные и случайные.

Разные источники угроз требуют разные методы и средства защиты информации, что в свою очередь также требует разработку методик и алгоритмов оценки риска угроз. Данный процесс требует выполнения ряда условий:

Первое условия, построение гибких моделей защиты информационных системы, что позволяет быстро и безопасно вносить нужные поправки.

Второе, в связи с огромным количеством факторов риска, математическая модель должна включать разработку эффективных численных алгоритмов в информационных моделях.

Третье, прозрачные и простые для понимания методы и алгоритмы оценки рисков информационной безопасности.

При оценке рисков информационной безопасности одним из главных этапов является выделение и анализ, основные угрозы и уязвимости. В настоящее время методы можно разделить на две группы [3].

К основным таким методам можно отнести:

1) количественный анализ рисков;

2) качественный анализ рисков.

Первый метод применяется в случаях, когда риски можно соотнести с конкретными количественными значениями, выраженными в материальной стоимости, процентах и др. Количественный метод позволяет получить конкретные значения оценки риска информационной безопасности [6]. В данном методе всем элементам оценки рисков присваивают определенные и реальные значения.

Данный метод имеет следующий алгоритм [1]:

1) определяется ценность конкретных информационных ресурсов в материальной стоимости;

2) проводиться оценка в количественном выражении потенциального ущерба в случаи удачной реализации угрозы;

3) определяется вероятность каждой угрозы;
4) определяется общий потенциальный ущерб;
5) проводится анализ после получение данных по каждой угрозе.

При втором подходе, объекту оценки присваивается показатель (например, по трехбалльной или десятибалльной шкале). Анализ рисков в качественном методе проводится с вовлечением сотрудников, имеющих данную компетенции в области информационной безопасности [4].

Алгоритм состоит из следующих пунктов:
1-3) первые три пункта схожи с количественным методом.
4) создается вывод об уровне риска и вероятности реализации каждой угрозы.
5) проводиться анализ полученных данных по каждой угрозе.
6) разрабатываются методы и средства безопасности, контрмеры и действия по каждой актуальной угрозе.

Появление новых угроз информационной безопасности и средств защиты приводят к необходимости выбора подходящего методы оценки, что зависит от конкретной области развития предприятия [7]. Разработка и применения моделей информационной безопасности на предприятиях, а также алгоритмов и методов являются необходимым условием для создания систем поддержки принятия решений по управлению информационной безопасностью на предприятии.

СПИСОК ЛИТЕРАТУРЫ

1. Анализ рисков информационной безопасности. – URL:https://bcoll.ru/564-analiz-riskov-informatsionnoj-bezopasnosti/ (дата обращения: 04.10.2020).
2. Информационной безопасности. Виды угроз и защиты информации. – URL:http://galyautdinov.ru/post/informacionnaya-bezopasnost (дата обращения: 04.10.2020).
3. Информационные риски: методы оценки и анализа. – URL: https://itportal.ru/science/economy/informatsionnye-riski-metody-otsenk/ (дата обращения: 04.10.2020).
4. Математическое моделирование информационной и экономической безопасности на предприятиях малого и среднего бизнеса. – URL: https://www.fundamental-research.ru/ru/article/view?id=32923 (дата обращения: 04.10.2020).
5. Основные понятия защиты информации и информационной безопасности. – URL: https://studref.com/322433/informatika/osnovnye_ponyatiya_zaschity_informatsii_informatsionnoy_bezopasnosti (дата обращения: 04.10.2020).
6. Технология оценки угроз и уязвимости. – URL: https://helpiks.org/6-33071.html (дата обращения: 04.10.2020).
7. *Цветкова О.Л., Заслонов С.А.* Имитационное моделирование зависимости информационной безопасности организации от области деятельности // Вестник Донского государственного технического университета. – 2017. – № 17(4). – С. 116-121. – URL:https://doi.org/ 10.23947/1992-5980-2017-17-4-116-121.

ANALYSIS OF METHODS FOR ASSESSING INFORMATION SECURITY RISKS AT THE ENTERPRISE

SAKHNO Vitaly Viktorovich
master student
Don State Technical University
Rostov-on-Don, Russia

Nowadays, almost every company is under the possibility of hacker attacks. Information protection plays an important role, the level of it depends on whether the company loses data, or telecommunications equipment breaks down, which threatens the company with large losses.
Key words: threats, information security, risk assessment, means of protection.