ГРАБЧУК О.П., ст. гр. ЭК-09б
Науч. рук.: Губенко Н.Е. к.т.н., доц.
Донецкий национальный технический университет,
г. Донецк

СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ПРЕДПРИЯТИЯ

Обоснована важность внедрения системы безопасности предприятия в рамках управления его производственно-экономической деятельности. Проанализированы основные методы защиты.

Актуальность. Современная Украина, как и другие государства, переживает бум развития информационных технологий. Очень трудно представить даже жизнь рядового гражданина без использования компьютерных технологий, а уж предприятие без применения новейших технологий работы с информацией обречено на провал. Компьютер помогает вести бухгалтерский и налоговый учет, хранить документацию, автоматизировать процесс производства или оказания услуг на любом современном предприятии. Но, в связи с развитием технологий, учащаются случаи нападения на информационные сведения о предприятии, что делает актуальным поиск методов защиты.

Таким образом, на сегодня управление предприятием – это решение двух основных задач: построения интегрированной информационной среды предприятия, где должны содержаться все знания и технологии, которые информационно поддерживают процесс производства, и обеспечения безопасности функционирования этой информационной системы (во избежание разглашения, утечки и порчи информации).

Цель исследования. Исследовать системы, которые могут анализировать риски. Их интеграция в информационное пространство предприятия обеспечивает нужные инструменты для организации системы управления безопасностью предприятия.

Основная часть. Анализ рисков – важнейшая часть комплексной оценки информационной безопасности предприятия. Риск описывает вероятный ущерб от утечки или порчи информации. Его можно охарактеризовать двумя значениями: вероятностью ущерба и величиной ущерба. Величина риска зависит от степени защищенности системы и оценивается либо в количественных показателях, либо в качественных (высокий, низкий и так далее).

Для упрощения процесса анализа рисков существует несколько систем. В данной статье будут рассмотрены такие системы анализа рисков: CRAMM, Risck Watch и ГРИФ. Все эти системы проводят единовременный анализ рисков, то есть для обеспечения большей точности анализа рисков необходима повторная организация процедуры

анализа.

Метод CRAMM (the UK Government Risk Analysis and Management Method) был создан в Великобритании по заданию правительства. Программный продукта, реализующий этот метод, производит фирма Insight Consulting Limited.

На сегодняшний день CRAMM – это очень мощный универсальный инструмент, который позволяет не только анализировать риски, но и выполнять некоторые аудиторские задания, например:

- обследование информационной системы и выпуск необходимой для этого процесса документации;
- проведение аудита;
- разработка политики безопасности предприятия и плана обеспечения непрерывности деятельности и так далее.

В основе метода CRAMM - комплексный подход к оценке рисков, сочетающий в себе как количественные, так и качественные методы анализа. Данные метод сравнительно универсален и подходит почти для всех предприятий, начиная от правительственного и заканчивая коммерческим сектором. Существуют различные версии, которые созданы для разных типов организаций, причем разница в этих версиях в основном в их базах знании.

Недостатки метода:

- слишком большое количество отчетов;
- высокая трудоемкость метода.

Программное обеспечение RiskWatch также является удобным средством для управления рисками. В семейство RiskWatch входит большое множество продуктов. Среди них программы, предназначенные для анализа информационных рисков, для обеспечения физических методов защиты, для оценки выполнения стандарта HIPAA и ISO17799.

Метод RiskWatch, в отличие от CRAMM, ориентирован на точную количественную оценку отношения потерь от угроз безопасности и затрат на создание системы защиты. При этом риски в сфере информационной безопасности компьютерной сети рассматриваются совместно с рисками в сфере физической безопасности компьютеров. А в основе данного метода находится методика анализа рисков, состоящая из четырех этапов: определяется предмет исследования; вводятся данные, которые описывают характеристики системы; производится количественная оценка всех показателей; генерируются отчеты.

Главные критерии для оценки рисков в методе RiskWatch – это предсказание годовых потерь и оценка возврата от инвестиций. Это помогает провести анализ рисков и обосновать выбор мер и средств для защиты предприятия.

Метод RiskWatch ориентирован на анализ рисков на программно-техническом уровне защиты. Очень сложно осуществить комплексный

подход к обеспечению безопасности, используя полученные этим методом оценки. Основные недостатки RiskWatch:

- эффективно использовать в случаях, где не нужно учитывать организационные и административные факторы;
- не учитывается комплексный подход к информационной безопасности;
- программный продукт еще не русифицирован;
- высокая стоимость лицензии.

ГРИФ – это разработка российской компании Digital Security. С помощью этого метода можно дать сравнительно точную оценку рисков, существующих в системе, и провести глубокий анализ особенностей практической реализации информационной системы. Программа предназначена для применения руководителями предприятия и системными администраторами и имеет дружественный интерфейс.

Основной задачей системы ГРИФ является оценка уровня рисков в информационной системе, анализ эффективности существующей практики обеспечения безопасности предприятия и обоснование необходимости денежных вложений. В результате будет сформирована полная модель информационной системы с точки зрения безопасности информации, после чего можно проводить комплексную оценку рисков.

Основные недостатки ГРИФ:

- нет привязки к бизнес-процессам;
- невозможно сравнивать отчеты по разным этапам внедрения системы.
- невозможно добавить специфичные требования к политике безопасности

Вывод. Таким образом, оценка рисков утечки и порчи информации является очень важным элементом процесса управления предприятием. Для осуществления этого процесса существует большое количество приложений. Наиболее популярные из них: CRAMM, Risck Watch и ГРИФ. Каждый из этих методов имеет свои достоинства и недостатки и может быть использован в любом предприятии.

Библиографический список

1. Прохоров С.А., Федосеев А.А., Иващенко А.В.. Автоматизация комплексного управления безопасностью предприятия.- Самара, 2008.

2. Медведовский И. Современные методы и средства анализа и контроля рисков информационных систем компаний // iXBT.com.

3. Куканова Н. Современные методы и средства анализа и управление рисками информационных систем компаний // http://citforum.ru.