УПРАВЛЕНИЕ РИСКАМИ В КОРПОРАТИВНЫХ СЕТЯХ

Бабенко Ф.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ширинский В.П. – к.т.н., доцент

В работе проведен анализ основных подходов к оценке рисков информационной безопасности в корпоративных информационных сетях.

На современном этапе развития общества, когда информационную эру сменяет цифровая, глобальным трендом становится цифровизация предприятий. Технологически цифровизация базируется на масштабируемой облачной платформе и безопасной и стабильной корпоративной сети телекоммуникаций, обеспечивающей разнообразные сетевые сценарии. При этом, поскольку корпоративные сети телекоммуникаций обеспечивают технологические процессы предприятия, основным приоритетом является их надежность и информационная безопасность (ИБ) в них. Очевидно, что цифровизация предприятия может быть успешной только в том случае, если облако и сеть будут в состоянии гарантировать безопасность корпоративных данных. Вместе с тем, подключение корпоративной сети к облачной платформе, внешним сетям, использование гаджетов и электронных сервисов потенциально приводят к ее уязвимости. Все это делает проблему защиты информации и обеспечение ИБ в корпоративных сетях телекоммуникаций в целом и задачу определения рисков ИБ в этих сетях в частности крайне актуальными. При этом на первый план выходит создание быстродействующих методик как для оценки рисков ИБ в целом, так и локальных индикаторов состояния ИБ.

Информационная безопасность – это защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры. Информационная безопасность не сводится исключительно к защите информации. Поломки обслуживающей системы и задержки в ее работе также могут принести убытки.

В нашем конкретном случае под поддерживающей инфраструктурой понимается вычислительная сеть, которая, по сути, и является объектом нашего исследования. Сеть есть подвид информационной системы, безопасностью которой принято считать состояние защищённости системы, при котором обеспечивается доступность, конфиденциальность и целостность её ресурсов. В этом определении включены все три понятия, называемые «Триадой информационной безопасности»: Конфиденциальность – сохранение в секрете критичной информации, доступ к которой ограничен узким кругом пользователей (отдельных лиц или организаций). Целостность – свойство, при наличии которого информация сохраняет заранее определенные вид и качество. Доступность – такое состояние информации, когда она находится в том виде, месте и времени, которые необходимы пользователю, и в то время, когда она ему необходима.

Стоит отметить, что любая система управления ИБ ТК имеет свою техническую и организационную составляющую. Рассмотрим основную методику работы системы ИБ, применяемую в ТК на сегодняшний день. Как правило, основным техническим звеном системы управления ИБ в ТК является – подсистема ИБ, которая является органичной частью автоматизированных ИС ТК (к примеру, биллинговых). В рамках подсистемы ИБ функционируют средства защиты от несанкционированного доступа, средства криптографической защиты, средства антивирусной защиты, средства мониторинга эффективности защиты.

В рамках организационной составляющей выполняются следующие функции управления:

– организация и оперативное решение задач по защите информации;

– подбор и руководство кадрами по защите информации;

– материально-техническое обеспечение решения задач по защите информации (приобретение установка и наладка программных и технических средств защиты информации);

– контроль состояния защищенности автоматизированных ИС ТК и планирование мероприятий по защите автоматизированных ИС и развитию подсистемы ИБ;

– проведение мероприятий по повышению защищенности ИС ТК и развитию подсистем ИБ, включая управление проектами по внедрению сложных систем и проведение комплексных мероприятий по защите информации.

Задачей данной работы является разработка методов оценки риска и защищённости сетей, Для реализации потребуется следующее:

– учесть топологию сети;

– учесть параметры оборудования всех составных частей;

– учесть приоритеты и пожелания пользователя (пользователь – это тот, кто задаёт сеть, подлежащую аудиту и/или оптимизации);

– разработать математическое представление атакующих действий, их зависимостей и комбинаций;

– разработать методы вычисления риска и защищённости, а также алгоритма подбора параметров, оптимизирующих эти метрики.

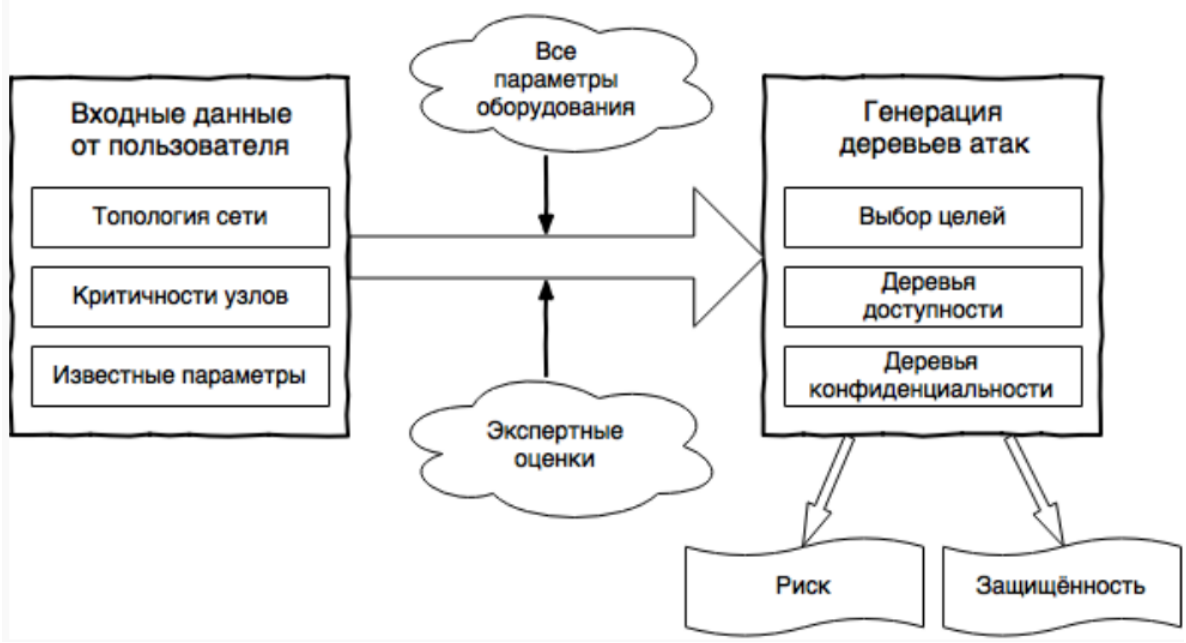

Рисунок 1 – Общая схема предлагаемого расчёта уровня риска и критичности

Список использованных источников:

1. Конеев, И.Р, Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с

2. Аникин И.В. Управление внутренними рисками информационной безопасности корпоративных информационных сетей // Научно-технические ведомости Санкт- Петербургского государственного политехнического университета. Информатика. Телекоммуникации. Управление. 2009. Т. 3. № 80. С. 35-40.

3. Аникин И.В. Метод оценки внутренних рисков информационной безопасности кор- поративных информационных сетей // Информация и безопасность. 2014. Т. 17. № 2. С. 320-323..