Голева Алина Игоревна
студентка
Ступко Кристина Олеговна
студентка
Мироненко Ольга Евгеньевна
студентка

Омский Государственный Технический Университет
г. Омск, Омская область

Анализ рисков информационной безопасности

Аннотация: *статья посвящена вопросу обеспечения информационной безопасности организации, вводится понятие анализа рисков, детально рассмотрены составляющие анализа рисков, рассмотрены методики оценки рисков, показана значимость анализа рисков для поддержания информационной безопасности организации.*

Ключевые слова: *анализ, информация, риски, безопасность, угроза, уязвимость.*

В XXI веке в связи с ускоренным развитием информационных технологий информация становится стратегическим ресурсом, производительной силой организации, что вызывает у ее собственника стремление получить преимущество за счет овладения информацией, а у конкурента – стремление нанести ущерб информационным ресурсам оппонента. Поэтому успешность и непрерывность бизнеса существенным образом зависит от обеспечения и совершенствования информационной безопасности.

Выбор системы информационной безопасности зависит от вида циркулирующей на предприятии защищаемой информации: при наличии сведений, составляющих государственную тайну, – обязательно исполнение нормативных требований и применение сертифицированных средств защиты; если же необходимо ограничить распространение информации, составляющей коммерческую и профессиональную тайну (к примеру, банковскую), – процесс построения системы защиты должен основываться на анализе рисков.

Анализ рисков – это комплексный подход к оценке защищенности системы с представлением результатов в виде количественных или качественных показателей.

В процессе анализа рисков оцениваются уязвимости и угрозы информационной системы, их критичность и величина ущерба для компании, а также вырабатываются контрмеры по минимизации рисков.

Существует множество методик анализа рисков. Некоторые из них выполнены в виде специализированных программ, что позволяет уменьшить трудоемкость анализа рисков и выбора контрмер. Примером программных методик является продукт CRAMM.

Другие же методики основаны на табличных методах, где наглядно отражается связь факторов негативного воздействия (угроз и уязвимостей) и вероятностей реализации угрозы с учетом показателей уязвимостей, а также их влияние на оценку риска.

Оценка рисков может производиться по двум или по трем факторам.

В первом случае риск определяется вероятностью реализации угрозы и величиной ущерба: $R = P_Y \cdot S$. Во втором случае оценка риска связана с тремя факторами: угроза, уязвимость, величина потери $R = P_{óãðîçû} \cdot P_{óÿçâèìîñòè} \cdot S$. То есть в данном случае вероятность реализации конкретной угрозы связана с вероятностью использования существующей в системе уязвимости для осуществления данной угрозы.

Вероятности, как в первом, так и во втором случае, могут быть оценены количественно (с помощью шкалы численных значений) или качественно (с помощью шкалы с градуированными уровнями: высокий, средний, низкий). Также существуют объективные и субъективные оценки вероятности. В качестве объективной оценки выступает относительная частота появления какого-либо события в общем объеме наблюдений, или иными словами - отношение числа благоприятных исходов к общему количеству наблюдений.

Объективная оценка применяется при анализе результатов большого числа наблюдений, имевших место в прошлом, при этом очевидно неудобство использования данного метода оценки, так как должен быть собран весьма обширный материал об инцидентах в этой области, а это невозможно, если компания использует новейшее оборудование и технологии, для которых еще нет достоверной статистики.

Под субъективной оценкой вероятности подразумевают меру уверенности человека в том, что данное событие произойдет. Часто в методиках анализа рисков используют субъективные критерии, так как считается, что оценка должна отражать точку зрения владельца информационных ресурсов.

Для оценки рисков должны быть выбраны шкалы для вероятностей события, для критичности инцидента, а также шкала уровня риска.

Приведем пример оценки риска для двухфакторной модели.

1. Определим субъективную шкалу вероятностей событий:

A – событие почти никогда не происходит;

B – вероятность события стремится к 0,5;

C – событие почти обязательно должно произойти;

2. Определим субъективную шкалу критичности инцидентов:

Min – незначительное происшествие: последствия легко устранимы,

затраты на ликвидацию последствий отсутствуют или невелики;

Average – происшествие с умеренными результатами: ликвидация последствий не связана с крупными затратами;

Max – происшествие приводит к значительными затратами или невозможности решения критически важных задач.

Риск, связанный с конкретным событием, зависит от двух факторов и может быть определен как в таблице 1.

Таблица 1

Определение риска

	Min	Average	Max
A	Низкий риск	Низкий риск	Средний риск
B	Средний риск	Средний риск	Высокий риск
C	Средний риск	Высокий риск	Высокий риск

Напомним, что это пример, и при оценке риска шкалы и таблица в зависимости от требуемой детализации могут быть построены иначе, иметь другое число градаций.

После оценки рисков можно выбрать средства, обеспечивающие необходимый и достаточный уровень информационной безопасности компании (контрмеры, позволяющие снизить уровень рисков). При этом важно помнить один из основополагающих принципов защиты информации: затраты на построение и модернизацию системы безопасности не должны превышать стоимость активов (значимых для бизнеса информационных ресурсов) компании.

Система защиты должна быть комплексной, то есть содержать контрмеры разных уровней обеспечения безопасности: организационного, физического (для предотвращения несанкционированного доступа) и программно-аппаратного.

Для выбора из множества существующих контрмер подмножества необходимых в различных методиках используются таблицы, в которых уровням угроз соответствуют возможные контрмеры.

Таким образом, в процессе анализа рисков необходимо классифицировать активы компании по степени их значимости, определить их критичность (величину потерь в случае реализации угроз безопасности актива), затем определить возможные источники проблем (угрозы и уязвимости), провести оценку рисков, исходя из заданных шкал с уровнями угроз и вероятностей событий, и, наконец, подобрать контрмеры, позволяющие минимизировать риски информационной безопасности.

В заключении хотелось бы отметить, что в настоящее время недооценка важности анализа рисков компании для непрерывности бизнеса может привести к колоссальным материальным и имиджевым потерям. Анализ и управление рисками информационной безопасности постепенно становятся повседневной реальностью для все большего числа компаний. И это безусловно правильное решение, так как для любой организации, какой бы сферой деятельности она не занималась, анализ рисков, идентификация уровня его критичности – первый шаг для осуществления грамотного управления рисками, что означает своевременное выявление и регулирование тех рисков, которые могут угрожать имуществу и доходу компании.

Список литературы

1. Астахов А.М. Искусство управления информационными рисками. / А. М. Астахов. – Москва: ДМК Пресс, 2010 – 312 с.

2. Петренко С. А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. - М.: Компания АйТи; ДМК Пресс, 2004 - 384 с.