Козлов А.Д., Нога Н.Л.

Оценка рисков информационной безопасности с учетом фактора времени

Аннотация: Предложена методика оценки рисков информационной безопасности, учитывающая фактор времени.

Ключевые слова: риск, субъективные факторы, функция риска, скорость изменения риска, темп прироста риска, динамическое управление риском

В настоящее время широкое внедрение цифровых технологий в различных областях человеческой деятельности способствует как развитию отдельных отраслей экономики, так и бурному росту такого рода услуг как цифровые услуги.

Любой процесс в бизнесе, если упрощенно, зависит от затрат; характеристик услуг или продуктов, являющихся результатом процесса; качества производимых услуг или продуктов; рисков, связанных с этим процессом и реализацией продуктов. Т.е. риски, в том числе риски информационной безопасности, являются неотъемлемой частью объекта управления бизнес-процессом.

На текущий момент существует множество методик анализа и оценки рисков. Рассмотрим некоторые, наиболее распространенные из них. **Coras** [1]: данная методика применяется для проведения только разовых оценок, нет периодичности В то же время положительным аспектом является бесплатность ее программного приложения и легкость в установке и применении. **OCTAVE** [2]: при этой методике оценки рисков информационной безопасности проводятся регулярно, используется в качестве способов снижения рисков (но не исключения). Методика дает качественную оценку рисков, но эта оценка может быть использована для определения количественной шкалы при проведении ранжирования. По этой методике затруднительно проводить мониторинг состояния рисков. **CRAMM** [3]: также как и в OCTAVE используется в качестве способов снижения рисков. Методология использует как качественные, так и количественные оценки рисков. Отсутствует мониторинг способов управления остаточными рисками и перерасчет максимально допустимых значений рисков. Основной недостаток при практическом применении – необходимость

привлечения высококвалифицированных специалистов. В работе авторов [4] была предложена методика оценки рисков обеспечения информационной безопасности при использовании облачных технологий в информационных системах корпораций, в отличие от вышеперечисленных методологий, на основе методов нечеткой логики с учетом субъективных факторов риска. Практическая реализация предполагает использование пакета Fuzzy Logic Toolbox системы Matlab [5]. Программный пакет дает возможность периодически и в любое время обновлять величины рисков. Кроме того, методика позволяет учитывать субъективные факторы риска, присущие практически любой организации.

В работе [4] авторами была представлена формула для вычисления риска информационной безопасности системы R_1 с учетом субъективных факторов

$$R_1 = \frac{R(p(T), p(V), D)}{K_c}, \quad (1)$$

где $p(V)$ - вероятность использования конкретной уязвимости, $p(T)$ - вероятность реализации угрозы через данную уязвимость, D - величина значения возможного ущерба от реализации данной угрозы и K_c - коэффициент уровня контроля информационных ресурсов, характеризующий субъективные факторы и принимающий значения в интервале (0, 1).

Практически во всех методологиях, как в вышеперечисленных, так и в других, не рассматриваются вопросы изменения значений рисков во времени, хотя вопросы мониторинга поднимаются.

Однако необходимо отметить, что и вероятность использования конкретной уязвимости, и вероятность реализации угрозы через данную уязвимость, а также значения возможного ущерба зависят от времени. Например, чем дольше остается не устраненной выявленная уязвимость, тем выше вероятность ее использования злоумышленниками и вероятность реализации через нее угрозы.

Также от времени может зависеть и возможный ущерб. Так, при реализации определенной угрозы может происходить утечка конфиденциальной информации (sensitive information), и чем дольше существует данная уязвимость, тем больше может быть ущерб. Кроме этого, для большинства информационных систем характерно накопление данных и соответственно увеличение со

временем ценности информационных ресурсов, а также рост числа пользователей, для которых потеря доступности ресурсов может быть связана с финансовыми потерями.

В этой связи предлагается ввести функцию риска $R_1 = R_1(t)$, (где R_1 из (1)) т.е. попробовать проанализировать риски в зависимости от времени. Для этого было бы достаточно найти производную функции $R_1(t)$, что, на наш взгляд, может оказаться достаточно сложной задачей в условиях большой неопределенности. Зная скорость изменения риска, можно определить значение риска через какой-то промежуток времени (в который, например, не устранили брешь в системе защиты информационной системы, т.е. уязвимость). В случае сложности дифференцирования функции риска можно рассмотреть следующий показатель: T_{ri} - темп прироста риска (в процентах). Т.е., если в начальный рассматриваемый момент времени t_0 значение риска $R(t_0)$, а в момент времени t_1 - $R(t_1)$, то темп прироста равен

$$T_{ri} = \frac{R(t_1) - R(t_0)}{R(t_1)} \times 100 - 100. \qquad (2)$$

Если теперь воспользоваться таблицей значений риска, приведенной в работе [4]

№ п/п	Уровень риска	Границы терма «Риск»
1	Незначительный	0-0,20
2	Допустимый	0,16-0,50
3	Высокий	0,45-1,00

и используя темп прироста риска из (2) на определенном промежутке времени, можно получить значение риска в конце промежутка времени и увидеть в соответствии с таблицей его уровень. Таким образом, можно определить момент времени, когда уровень риска превысит допустимый уровень. Это, в свою очередь, позволяет своевременно принять все возможные меры для снижения уровня риска.

Используя показатель темпа прироста риска, получая значение риска практически в любой момент времени, фактически можно перейти от периодической оценки риска к динамическому управлению риском информационной безопасности в организации.

Литература:

1. The CORAS Method [Электронный ресурс]. – Режим доступа: www.coras.sourceforge.net/index.html. – (Дата обращения: 05.09.2019).
2. *Алексеев, Е.Р., Чеснокова, О.В.* Введение в Octave для инженеров и математиков. – М.: ALT Linux, 2012. – 308 с.
3. *Разумников С.В.* Анализ возможности применения методов OCTAVE, RiskWatch, CRAMM для оценки рисков ИТ для облачных сервисов // Современные проблемы науки и образования, – 2014. – № 1. – С. 247-248.
4. *Козлов, А.Д., Нога, Н.Л.* Риски информационной безопасности корпоративных информационных систем при использовании облачных технологий // Управление риском, – 2019. – № 3. – С. 31-46.
5. Matlab версия 9.6.0 R2019a [Электронный ресурс]. – Режим доступа: https://1progs.ru/matlab / – (Дата обращения: 05.09.2019).