МЕТОДИКА ОЦЕНКИ СОВОКУПНОЙ ЦЕННОСТИ ИНФОРМАЦИОННЫХ АКТИВОВ ПРИ ОЦЕНКЕ РИСКОВ ОТ ИНСАЙДЕРСКИХ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

METHOD OF ESTIMATING THE TOTAL VALUE OF INFORMATION ASSETS WHEN ASSESSING THE RISKS FROM INSIDER THREATS TO INFORMATION SECURITY

M. Polyanichko

Summary. Insider threats to information security are threats from employees of the organization. The article addresses the problem of information security risks assessment related to the activity of insiders. A method of assessing the total value of information assets, expanding the ability to assess the potential consequences of the actions of the insider is introduced.

Keywords: insider, insider threat, detection and insider counteraction, risk assessment

Поляничко Марк Александрович
К.т.н., доцент, ФГБОУ ВО ПГУПС (г. Санкт-Петербург)
polyanichko@pgups.ru

Аннотация. Инсайдерские угрозы информационной безопасности — это угрозы, исходящие от работников организации. В статье рассматривается проблема оценки рисков информационной безопасности, связанных с деятельностью инсайдеров. Предложена методика оценки совокупной ценности информационных активов, расширяющая возможности по оценке потенциальных последствий от действий инсайдера.

Ключевые слова: инсайдер, инсайдерская угроза, обнаружение и противодействие инсайдерам, оценка риска.

Цифровизация различных сфер деятельности [9] приводит к росту инцидентов информационной безопасности, связанных с деятельностью инсайдеров [3]. Инсайдерские угрозы несут разносторонний и значительный риск для организаций, так как действия инсайдеров могут нести угрозу репутации, бренду и финансовому положению компании [6]. Данная ситуация требует развития подходов к противодействию деятельности инсайдеров, в том числе развития методов оценки рисков информационной безопасности, связанных с инсайдерскими угрозами. Риск часто характеризуется как возможность того, что данная угроза будет реализована и нанесет ущерб организации. В случае противодействия инсайдерам, для понимания возможных последствий от их действий требуется определение совокупной ценности информационных ресурсов, к которым они имеют доступ. В особенности в случае, когда рассматриваются ИТ работники, имеющие привилегированные учетные записи и администраторский доступ к базам данных.

Актуальной проблемой оценки рисков информационной безопасности является определение стоимости (ценности) информационных активов. Эта проблема проявляется особенно сильно в том случае, если для оценки рисков используются количественные методы, которые подразумевают наличие конкретной информации о стоимости активов. В данной работе принимается, что ценность актива проистекает возможности его использования для создания новых ценностей, продуктов и знаний, а также применения для реализации услуг бизнеса, который его использует. Имущество или активы могут быть разделены на нематериальные активы (знания, информация, данные и т.д.) и материальное имущество (оборудование и другие физические активы) [2].

К информационным активам можно отнести:

- Материальные информационные активы — компьютерная техника, компьютерные сети, носители информации, переносные электрические провода и др.
- Нематериальные активы — базы данных, системная документация, руководства пользователя, оперативных процедур, планов и т.д.
- Бумажные документы — контракты, инструкции, деловая документация, результаты деятельности и т.д.
- Программное обеспечение — прикладное и системное программное обеспечение, средства разработки и поддержки.
- Имидж и репутация компании.
- Корпоративная база знаний компании.

В настоящее время происходит активный рост ценности нематериальных активов. Растет значимость и влияние информационных активов на успешность бизнеса

Таблица 1. Опросный лист для оценки ценности информационного актива

№	Вопрос	Ответы	Балл ответа
1	Что произойдет, если этот информационный актив исчезнет?	Ничего особенного	0
		Незначительно снизится эффективность работы	1
		Без него возникнут сложности, но актив заменяемый	2
		Без актива возникнут новые ненужные расходы	3
		Произойдут большие задержки в работе и потребуется его замена	4
2	Сколько будет стоить замена информационного актива или создание нового?	Пренебрежительно мало	0
		Стоимость существует, но она низкая	1
		Значительные затраты	2
		Высокая стоимость	3
		Неприемлемо высокая стоимость	4
3	Что произойдет, если конкурент будет обладать такой же информацией?	Ничего	0
		Подобная информация конкурентам и так доступна	1
		Конкурент получит понимание важных процессов	2
		Конкурент сможет догнать организацию	3
		Конкурент сможет получить преимущество	4
4	Существуют ли обязательства по хранению информации и существуют ли юридические последствия в случае ее потери?	Не существуют	0
		Необходимо хранить информацию непродолжительное время	1
		Организация должна хранить информацию, но последствий за нарушение не существует	2
		Хранение обязательно и организация может столкнуться с наказанием за неисполнение	3
		Хранение обязательно и организация может столкнуться с серьезным наказанием за неисполнение	4
5	Теряется ли важность информации со временем?	Очень быстро	0
		Быстро	1
		После 1 года	2
		После нескольких лет	3
		Не теряется	4

Таблица 2. Уровни ценности информационных активов

Уровень	Диапазон баллов	Описание
Очень низкий	0–4	Информационный актив не имеет экономической ценности и может быть заменен с минимальными затратами.
Низкий	5–8	Информационный актив представляет небольшую ценность, а его потеря имеет небольшое влияние на деятельность организации.
Средний	9–12	Информационный актив важен, но может быть заменен. Потеря имеет умеренные последствия.
Высокий	13–16	Информационный актив особенно важен для организации и его уничтожение может иметь серьезные последствия для организации.
Очень высокий	17–20	Наиболее ценный информационный актив, потеря которого имеет комплексное влияние на организацию.

в целом. В связи с цифровизацией всех основных отраслей и предприятий, такая тенденции сохранится. В таких условиях определить ценность информационных активов становится сложно и, как правило, данная ценность определяется субъективно.

Однозначного решения задачи оценки ценности информационного актива не существует, так же, как и не существует универсального метода оценки, который можно применять в различных условиях. Тем не менее, существуют возможности, позволяющие дать оценку ценности информации на основе определенного набора критериев [5]. Далее будут рассмотрены параметры, определяющие ценность информационных активов и предложен подход к их оценке.

Определение стоимости нематериальных активов является обязательным условием при оценке рисков информационной безопасности. Простая констатация факта, что некоторый информационный актив является более важным, чем другие, не является достаточным обоснованием для выделения финансирования на обеспечение его информационной безопасности. Поскольку ценность актива необходимо определять более точно, то требуется принимать во внимание форму его представления, способы работы с ним и структуру характеристик, формирующих его ценность. Еще одна причина затруднения оценки ценности информационных активов заключается в том, что, как правило, конкретные количественные данные о влиянии оцениваемых активов на результаты деятельности организации отсутствуют.

Как и другие организационные активы, информационные активы имеют стоимость, которая может складываться из стоимости приобретения, хранения и поддержки, но, при этом, ценность информационная актива не обязательно может подчинятся экономическим законам и обладать некоторыми уникальными свойствами, значительно влияющим на стоимость. К таким свойствам можно отнести [1, 4]:

1. Информация может распространяться в неограниченном количестве
2. Ценность информации увеличивается по мере роста ее использования
3. Информация может терять ценность со временем
4. Ценность информации растет по мере роста ее точности
5. Ценность информации растет при ее объединении с другой информацией
6. Объем информации не обязательно увеличивает ее ценность
7. Информация — неистощаемый ресурс

На основании этих свойств предлагается опросный лист, позволяющий дать оценку ценности информационного актива:

На основании результатов информационный актив может быть отнесен к одному их пяти уровней ценности информационного актива.

$$W = \{w_1, w_2, \dots, w_m\}, \quad (1)$$

где
w_i — оценка стоимости информационного актива;
m — количество информационных активов.

Оценки совокупной ценности информационных активов, доступных пользователю u_i может быть получена по формуле:

$$CV_i = \frac{\sum_{j=1}^{m} a_{ij} * w_j}{\sum_{j=1}^{m} a_{ij}} \quad (2)$$

где

a_{ij} — наличие доступа у пользователя i к ресурсу j.

$$a_{ij} = \begin{cases} 1, & \text{доступ есть} \\ 0, & \text{доступ отсутствует} \end{cases},$$

w_i — оценка стоимости информационного актива, $w_j \in W$.

Обнаружение инсайдерских угроз — комплексная задача, которая в силу непредсказуемости человеческого поведения [7] не имеет определенного решения и, скорее всего, текущая тенденция сохранится и со временем количество инцидентов информационной безопасности, связанных с деятельностью инсайдеров будет только возрастать. Предложенная методика оценки совокупной ценности информационных активов может быть внедрена в процессы управления рисками организации [8]. Это позволит определить наиболее актуальные инсайдерские угрозы и применить меры, снижающие потенциальный ущерб от действий инсайдера.

ЛИТЕРАТУРА

1. Glazer R., Measuring the Value of Information: The Information Intensive Organisation, IBM Systems Journal, Vol 32, No 1, 1993.
2. Humphreys E. J., Guide to BS7799 Risk Assessment and Risk Management, British Standards Institution, London, 1998.
3. Insider Threat Report: 2018 — CA Technologies // CA Technologies URL: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (дата обращения: 18.07.2018).

4. Moody D., Walsh P. Measuring The Value Of Information: An Asset Valuation Approach // Seventh European Conference on Information Systems (ECIS'99). 1999. С. 1–17.
5. Sajko M., Rabuzin K., Bača M. How to calculate information value for effective security risk assessment // Journal of Information and Organizational Sciences. 2006. № 2 (30). С. 263–278.
6. Поляничко М. А., Королев А. И. Критерии классификации инсайдеров // Естественные и технические науки. 2018.— № 9., Выпуск (123).— 2018 — с. 149–151.
7. Поляничко М. А. Моделирование действий инсайдеров на основе аппарата информатики поведения // Естественные и технические науки. 2018.— № 12., Выпуск (126).— 2018 — с. 446–449.
8. Поляничко М. А. Модель зрелости процессов противодействия внутренним угрозам // Естественные и технические науки. 2018.— № 11., Выпуск (125).— 2018 — с. 452–456.
9. Распоряжение Правительства РФ от 28.07.2017 N1632-р «Об утверждении программы Цифровая экономика Российской Федерации"».

ВО ПГУПС