ФОРМИРОВАНИЕ ПОНЯТИЙНОГО АППАРАТА В ОБЛАСТИ ПРОТИВОДЕЙСТВИЯ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ

FORMATION OF DEFINITION COMPLEX FOR INSIDER COUNTERACTION SCOPE

M. Polyanichko

Summary. The article deals with the problem of the lack of a unified definition of an "insider". The definitions used in the international literature are analyzed, the key characteristics of insiders are highlighted. A unified definition of the insider is offered taking into account various aspects characterizing insider activity.

Keywords: insider, information security, internal threats, information theft, fraud.

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

Аннотация. В статье рассматривается проблема отсутствия единого понятийного аппарата в области противодействия инсайдерам. Приводятся и рассматриваются используемые в международной литературе определения, выделяются ключевые характеристики инсайдеров. Предлагается определение инсайдера, учитывающее различные аспекты, характеризующие инсайдерскую деятельность.

Ключевые слова: инсайдер, информационная безопасность, внутренние угрозы, кража информации, мошенничество.

Многие группы исследователей работают над проблемой обнаружения и предотвращения инцидентов информационной безопасности, связанных с деятельностью инсайдеров [6]. В исследованиях принимают участие как государственные структуры и образовательные учреждения, так и коммерческие организации. Тем не менее, несмотря на активные работы в этой области, до сих пор не выработано единое определение понятия «инсайдер» [7, 8]. Например, во многих работах, рассматривающих проблему инсайдерских угроз, определение инсайдера не приводится, так как подразумевается, что этот термин интуитивно понятен. В связи с этим, в отсутствие единого понятийного аппарата, многие исследования порождают собственное понимание инсайдерской угрозы, которое может быть специфическим для конкретного набора данных, ситуации, предубеждений и предположений. В результате могут возникнуть сложности в разработке новых методов противодействия инсайдерам и при применении разработанных методик противодействия инсайдерам в различных областях или отраслях. Помимо этого, ситуация осложняется существованием определений, которые могут прямо противоречить друг другу.

Разработка единого понятийного аппарата необходима для того, чтобы гарантировать, что выявленные угрозы действительно относятся к инсайдерским. Кроме того, благодаря разработке и использованию понятийного аппарата, можно сравнить различные подходы к обнаружению инсайдеров для выбора наилучшего подхода для обнаружения конкретного типа инсайдера.

В исследованиях, посвященных внутренним угрозам можно найти различные противоречивые определения инсайдера. В таблице 1 приводится сводка основных, наиболее часто используемых определений.

Рассмотрение приведенных определений позволяет обобщить и выделить некоторые ключевые характеристики, отличающие инсайдеров от посторонних лиц:

- Инсайдеры — это доверенные лица. Они, как правило, являются сотрудниками, но также могут быть подрядчиками, консультантами, временными помощниками и даже сотрудниками сторонних деловых партнеров, которые имеют официальные или неофициальные деловые отношения с организацией [5, 10]. Разница с внешним нарушителем заключается в том, что инсайдерам можно доверять, поскольку они считаются частью организации, могут подписать соглашение о конфиденциальности и/или предполагается, что они преследуют цели, которые отвечают интересам организации.
- Инсайдеры имеют законный доступ. Важно проводить различие между законным и санкционированным доступом. Например, технический специалист или уборщик может иметь законный доступ в помещения, но на самом деле может не иметь права просматривать документы, оставленные на столах. Законный доступ может привести к физическому доступу или доступу по сети (например, удаленный доступ).
- Инсайдеры обладают знаниями об информации, информационных системах и услугах, используемых в организациях [1, 3]. Эти знания не ограничиваются только обладанием информацией о имеющихся базах данных и информационных системах, но и подразумевают понимание ценно-

Таблица 1. Определения инсайдера

№	Определение	Источник
1.	«Любое лицо, имеющее доступ к информационным системам и сервисам, права в них или знания о них и действующее внутри периметра безопасности».	Бишоп [1]
2.	«[…] инсайдером является любое лицо, которому был предоставлен любой уровень доступа к информационной системе. […] Важно то, что после того, как пользователям было предоставлено какое-либо официальное явное право на информационную систему, они считаются инсайдерами.»	Баттс и соавт. [2]
3.	«[…] имеется в виду любые и все лица, которые имеют доступ к информации организации, включая как подрядчиков, временных работников и т.п.»	Кэрролл [3]
4.	«Инсайдер: кто-то с официальным доступом к компьютерам и сетям организации. Например, инсайдером может быть подрядчик, аудитор, бывший сотрудник, временный деловой партнер и многие другие.»	Предд и соавт. [10]
5.	«[…] инсайдерами обычно являются сотрудники, подрядчики и консультанты, временные помощники и даже персонал сторонних деловых партнеров и их подрядчиков, консультантов и так далее.»	Шульц [5]
6.	«Человек, пользующийся доверием и имеющий доступ к конфиденциальной информации и информационным системам»	Андерсон и соавт. [11]
7.	«Инсайдер — любой, кто работает внутри периметра безопасности»	Патзакис [12]
8.	«Законные пользователи, знакомые с информационными системами, которые злоупотребляют своими привилегиями и могут причинить значительный ущерб»	Чинчани [13]

Таблица 2. Ключевые характеристики определений

Определение	Учет характеристик					Итог
	Доверие	Законный доступ	Знания об ИС	Навыки	Мотивация	
1.	0	1	1	0	0	2
2.	0	1	1	0	0	2
3.	0	1	1	0	0	2
4.	0	1	1	0	0	2
5.	0	1	0	0	0	1
6.	1	1	1	0	0	3
7.	0	1	0	0	0	1
8.	0	1	1	0	0	2
Итог	1	8	6	0	0	—

сти информации, которая хранится в них, а также процедур и мер безопасности, которые были приняты для защиты информации. Поскольку инсайдеры знают о мерах и политиках безопасности, они имеют возможность их нарушать, оставаясь незамеченными. Существует ролевая классификация инсайдеров [4], в которой в качестве основного критерия используется уровень знаний о системе, которыми они обладают. Начиная от администраторов системы, которые имеют полные административные права до продвинутых пользователей, которые не имеют этих прав, но обладают существенными знаниями и правами внутри системы, и пользователей приложения, которые, скорее всего, способны злоупотреблять информацией, которая доступна из приложений, с которыми они работают.

Помимо перечисленных ключевых характеристик необходимо принять во внимание и учесть в разрабатываемом определении еще несколько особенностей, характерных для инсайдерских угроз:

- Инсайдеры должны обладать навыками, необходимыми для совершения противоправных действий. Таким образом, инсайдерам требуются не только знания об информации, информационных системах и услугах, используемых в организации, но и умения для реализации возможностей по злоупотреблению своим положением.
- В современных условиях связывание определения инсайдера с периметром безопасности становится практически невозможным, так как границы периметров организаций размываются в связи с ростом популярности мобильных и об-

лачных технологий, развитием VPN сетей, использования в работе аутсорсинга и субподрядчиков.

- Инсайдер должен личный интерес (мотивацию) к совершению злонамеренных действий. Данный интерес может выражаться как в получении материальных выгод, так и в удовлетворении эмоциональных потребностей.

Для анализа полноты существующих определений предлагается составить матрицу учета ключевых характеристик для каждого определения из таблицы 1.

На основе вышесказанного можно сделать вывод, что основными характеристиками инсайдера, которые учитываются в большинстве рассматриваемых определений являются наличие законного доступа и наличия знаний об информационных системах организации, а информация о наличии у нарушителя необходимых навыков и мотивации не учитывается ни в одном их определений.

Следовательно, разрабатываемое определение должно отражать все характеристики инсайдера. Также необходимо отметить, что помимо характеристик самого инсайдера при разработке определения необходимо учесть различные формы представления информации (электронную и физическую) и условия, в которых инсайдер действует, то есть правила безопасности организации, отраженные в политике безопасности или других локальных нормативных актах.

Таким образом предлагается следующее определение инсайдера: «Инсайдер — доверенный субъект, который имеет и использует возможность нарушить одно или несколько правил безопасности организации по отношению к информационному активу вне зависимости от формы его представления в личных интересах».

Формализовано понятие «инсайдер» может быть представлено в виде логического условия [9]:

$$Insider(emp_i) = \begin{cases} 1, emp_i \in EMP \wedge \exists event_i \notin R \wedge P \neq \emptyset \\ 0, иначе \end{cases}$$

где emp_i — работник,
$event_i$ — действие работника,
EMP — легитимные работники организации,
R — множество разрешенных действий,
P — личная выгода.

Для формирования понятийного аппарата, необходимо также привести определения понятий «инсайдерская угроза» и «инсайдерская деятельность».

Инсайдерская деятельность — открытые или скрытые единичные действия или последовательности действий инсайдеров, наносящие ущерб для организации.

Ущерб от инсайдерской деятельности — последствия, возникшие в результате действий инсайдера и выражающиеся в нанесении имущественных или моральных потерях для организации.

Инсайдерские угрозы — совокупность условий и факторов, создающих опасность возникновения инсайдерской деятельности в организации.

Инсайдерский инцидент информационной безопасности — одно или несколько зафиксированных событий информационной безопасности, вызванных инсайдерской деятельностью.

Предложенное определение может быть использовано при разработке подходов и методов противодействия инсайдерам, построения автоматизированных систем их обнаружения. Применение данного определения позволит унифицировать процессы управления инцидентами информационной безопасности, связанных с внутренними нарушителями и сравнивать их эффективность.

ЛИТЕРАТУРА

1. Bishop M., Gates C. Defining the insider threat // Proceedings of the 4th annual workshop on Cyber security and informaiton intelligence research developing strategies to meet the cyber security and information intelligence challenges ahead — CSIIRW '08. 2008. С. 1.
2. Butts J. W., Mills, R.F. & Baldwin, R.O. (2005). Developing an Insider Threat Model Using Functional Decomposition. In Proceedings of the Third international workshop on mathematical methods, models, and architectures for computer network security (St. Petersbur.
3. Carroll M. D. (2006). Information Security: Examing and Managing the insider Threat. In Proceedings of the 3rd annual conference on Information security curriculum development, Kennesaw, Georgia (USA).
4. Furnell S., Phyo A. H. Considering the Problem of Insider IT Misuse // Australian Journal of Information Systems. 2003. № 2 (10). С. 134–138.
5. Schultz E. E., «A framework for understanding and predicting insider attacks», Computers & Security, vol. 21, pp. 526–531, 2002.
6. Поляничко М. А., Королев А. И. Подход к выявлению инсайдерских угроз в организации // Естественные и технические науки. 2018.— № 9., Выпуск (123).— 2018 — с. 152–154.
7. Поляничко М. А. Предметно-ориентированная онтология представления инсайдерской угрозы // Естественные и технические науки. 2018.— № 12., Выпуск (126).— 2018 — с. 453–458.

8. Поляничко М. А., Королев А. И. Критерии классификации инсайдеров // Естественные и технические науки. 2018.— № 9., Выпуск (123).— 2018 — с. 149–151.
9. Поляничко М. А. Модель среды возникновения инсайдерской угрозы // Естественные и технические науки. 2018.— № 12., Выпуск (126).— 2018 — с. 449–453.
10. L. Pfleeger, J. B. Predd, J. Hunker, and C. Bulford. 2010. Insiders behaving badly: addressing bad actors and their actions. IEEE Transactions on Information Forensics and Security 5, 1 (2010), 169–179.
11. R. Brackney, R. Anderson. Understanding the insider threat: Proceedings of a march 2004 workshop. Technical report, RAND Corporation, Santa Monica, CA, March 2004.
12. J. Patzakis. New incident response best practices: Patch and proceed is no longer acceptable incident response. Technical report, Guidance Software, Pasadena, CA, September 2003.
13. R. Chinchani, D. Ha, A. Iyer, H. Q. Ngo, and S. Upadhyaya. 2010. Insider threat assessment: Model, analysis and tool. In Network Security. Springer, 143–174. 2010. C. 2010.

Журнал «Современная наука: актуальные проблемы теории и практики»

Петербургский государственный университет путей сообщения Императора Александра I