DOI 10.25586/RNU.V9187.18.09.P.139 УДК 004.056.5, 004.89

В.А. Минаев, Б.Н. Коробец, Е.В. Вайц, Ю.И. Стрельников

КОНЦЕПТУАЛЬНОЕ МОДЕЛИРОВАНИЕ ИНСАЙДЕРСКОЙ ДЕЯТЕЛЬНОСТИ В СИСТЕМАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Показано, что инсайдерские угрозы стали серьезной проблемой для компаний, требуя создания системного инструментария для своего анализа, прогнозирования и управления. Из анализа статистических показателей делаются два вывода, важных для создания концептуальных моделей инсайдерской деятельности. Первый – необходимо описать сложную систему информационного взаимодействия между всеми участниками корпоративного процесса в компании, учитывающего предпринимательские, психологические, финансово-экономические и иные риски и мотивы. Второй – следует разработать стратегию защиты, которая сочетает организационные и программно-технические средства и методы, включая системы предотвращения утечек данных (DLP-системы). При концептуальном моделировании одной из важных задач при построении системы защиты (СЗ) компании является создание поведенческих моделей инсайдера-нарушителя на основе визуализации информации. В качестве метода визуализации поведения целесообразно использовать системно-динамические модели. Рассматриваются угрозы кражи информации инсайдером. Дана классификация типов инсайдеров, подразделяемых на две категории – лояльные и злонамеренные. Приведены подробные сведения об умысле, мотивации и действиях каждого из перечисленных типов. Используя платформу имитационного моделирования Anylogic, визуализировали системы основных элементов поведения инсайдера и их взаимодействия применительно к двум случаям: когда он действует в одиночку и когда ему помогают сообщники. Представлены соответствующие диаграммы причинно-следственных связей.

***Ключевые слова*:** *инсайдер, угроза, информационная безопасность, концептуальная модель, имитационная система.*

V.A. Minaev, B.N. Korobets, E.V. Weitz, J.I. Strelnikov

CONCEPTUAL MODELING INSIDER ACTIVITIES IN INFORMATION SECURITY SYSTEMS

It is shown that insider threats have become a serious problem for companies, requiring the creation of system tools for their analysis, forecasting and management. From the analysis of statistical indicators, two conclusions are drawn that are important for the development of conceptual models of insider activities. First, it is necessary to describe a complex system of information interaction between all participants of the corporate process in the company, taking into account business, psychological, financial, economical and other risks and motives. Second, a protection strategy that combines organizational and programmatic and techniques tools, including data leakage prevention (DLP-systems), should be developed. In conceptual modeling, one of the important tasks in the construction of company security system (SS) is to create of insider's behavioral models based on visualization of information. It is advisable to use system-dynamic models as a method of behavior visualization. The threats of information theft by an insider are considered. The classification of insiders types, divided into two categories – loyal and malicious – is done. Details about the intent, motivation, and actions of each of these types are given. Using the AnyLogic simula-

tion modeling platform, visualization of the system of insider behavior basic elements and their interaction is carried out in relation to two cases: when it acts alone, and when it is assisted by accomplices. The corresponding diagrams of cause-and-effect relationships are presented.

Keywords**:** *insider, threat, information security, conceptual model, simulation system.*

Введение

Инсайдерские угрозы в последние годы приобрели характер серьезной проблемы при решении задач обеспечения информационной безопасности компаний, требуя разработки системного инструментария для своего анализа, прогнозирования и управления.

Распределение инсайдерских угроз в российских компаниях по их источникам [1] представлено на рис. 1.

Из рис. 1 следует, что наибольший вклад в инсайдерские угрозы, как и ожидалось, вносят действующие сотрудники (66%), внешние злоумышленники, занимая второе место, создают 29,7% вносимых угроз. Далее, отличаясь на порядок, располагаются в порядке убывания угрозы со стороны подрядчиков, бывших сотрудников, руководителей и системных администраторов (в общей доле – 4,3%).

Если говорить о распространенности самих инсайдерских угроз, то в своем большинстве они проявляются в виде утечки данных и искажениях в документации, примерно по четверти от их количества составляют утрата информации и сбои в работе информационных систем, по одной пятой – кражи оборудования и саботаж, и, наконец, не более 10–15% другие внутренние угрозы [2]. При этом до 80% информации, на которую посягают инсайдеры, – персональные данные и платежная информация.

Из анализа приведенных показателей можно сделать два вывода, важных для создания эффективных моделей инсайдерской деятельности.

Первый – основное внимание при концептуальном обосновании моделей необходимо обратить на возможность описания системы информационного взаимодействия между всеми участниками корпоративного процесса в компании, учитывающего предпринимательские, психологические, финансово-экономические и иные риски и мотивы.

Второй – для максимального снижения вероятности реализации инсайдерских угроз и минимизации их последствий необходимо разработать такую стратегию защиты, которая органично сочетает организационные и программно-технические средства и методы.

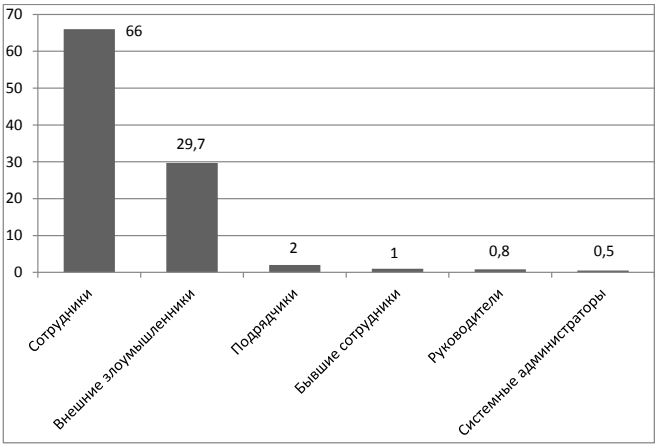

Рис. 1. Распределение инсайдерских угроз в российских компаниях по их источникам, %

Говоря об *организационных мерах*, необходимо отметить, что они охватывают широкий спектр методов противодействия инсайдерской деятельности и разрабатываются в зависимости от типа информации, используемой в работе организации. К организационным мерам предупреждения инсайда относят и работу с персоналом на этапах приема на работу, в ходе работы в должности, при увольнении. Работа с кадрами включает оценку благонадежности кандидатов, анализ психофизических типов работников, повышение их лояльности и т. д.

Программно-технические меры против инсайдерских действий предполагают применение систем предотвращения утечек данных – Data Loss Prevention системы (DLP-системы), – обеспечивающих высокий уровень защиты информации.

Говоря о модели предметной области – противоправной деятельности инсайдеров, подчеркнем, что процесс ее моделирования начинается с выявления абстракций, существующих в реальном мире формирования и реализации злонамеренных планов внутренних нарушителей информационной безопасности (ИБ) организаций. Поэтому первый этап моделирования заключается в создании концептуальной модели инсайдерской деятельности, которая отражает семантику предметной области в виде совокупности понятий (сущностей), их характеристик (атрибутов) и связей (ассоциативных отношений между сущностями).

При концептуальном моделировании предметной области [3] одной из важных задач при построении системы защиты (СЗ) организации является создание поведенческих моделей инсайдера-нарушителя на основе визуализации информации, которая легко воспринимается, позволяя лучше понять причинно-следственные особенности и динамику развития потенциального внутреннего инцидента ИБ.

Опыт авторов показал, что в качестве метода для визуализации поведения внутреннего нарушителя ИБ (инсайдера) целесообразно использовать системно-динамические модели [4], предполагающие разработку ориентированного графа исследуемой системы на базе статистических данных ее функционирования или экспертного мнения о ее поведении.

Поведение инсайдера существенно отличается в зависимости от того, какую угрозу ИБ он реализует. Поэтому целесообразно производить моделирование каждой внутренней угрозы ИБ в отдельности. В качестве угрозы в данной статье рассматривается угроза кражи информации инсайдером.

Классификация типов инсайдеров

Выделим в соответствии с рекомендациями работ [5; 6] шесть типов инсайдеров: «халатный» и «манипулируемый» – из категории лояльных, а также «обиженный», «нелояльный», «подрабатывающий» и «внедренный» – из категории злонамеренных. В таблице приведены более подробные сведения об умысле, мотивации и действиях каждого из перечисленных типов. Рассмотрим кратко характеристику каждого из представленных в таблице типов инсайдеров. Группу лояльных нарушителей составляют «халатные» и «манипулируемые» инсайдеры.

Классификация типов инсайдеров

Тип инсайдера	Умысел	Корысть	Кем ставится задача	Действия
Халатный	нет	нет	никем	сообщение
Манипулируемый	нет	нет	никем	сообщение
Обиженный	да	нет	самостоятельно	отказ
Нелояльный	да	нет	самостоятельно	имитация
Подрабатывающий	да	да	самостоятельно/извне	отказ/имитация/взлом
Внедренный	да	да	извне	взлом

«Халатный» (известен и как «неосторожный») – является наиболее распространенным типом инсайдера. Как правило, такие сотрудники относятся к рядовому составу и нарушения с его стороны в отношении конфиденциальной информации носят немотивированный характер, не имеют конкретных целей, умысла, корысти. Самые частые инциденты с их участием – вынос конфиденциальной информации из расположения компании для работы с ней дома, в командировке, утеря носителя или доступ посторонних к этой информации. Несмотря на отсутствие зловредных намерений, ущерб от подобных утечек может быть сравним с промышленным шпионажем. Против таких лояльных нарушителей действенными являются простые технические средства предотвращения каналов утечек: контентная фильтрация исходящего трафика в сочетании с контролем устройств ввода/вывода.

«Манипулируемый» инсайдер используется для получения обманным путем персональной информации: паролей, пин-кодов, номеров кредитных карт, адресов и т. п. Например, путем телефонного правдоподобного запроса конфиденциальных данных от «авторитетного» лица. Кем на самом деле является звонивший, остается только догадываться.

Злонамеренные нарушители, в отличие от сотрудников, описанных выше, осознают, что своими действиями они наносят вред компании, в которой работают.

«Обиженные» (по существу – саботажники) – это сотрудники, стремящиеся по личным мотивам (недостаточный размер материальной компенсации, неподобающий статус в корпоративной иерархии, отсутствие моральной мотивации) нанести, в частности, «информационный» вред своей компании. При этом, исходя из собственных представлений о наносимом вреде, они определяют, какую информацию похитить и кому ее передать – пресса, криминальные структуры и т. п.

«Нелояльные» инсайдеры – это прежде всего сотрудники, принявшие решение сменить место работы или решившие открыть собственный бизнес. Стало обычным, что уходящий сотрудник коммерческого отдела уносит с собой копию базы клиентов, а финансового – финансовой базы. Увеличивается количество инцидентов, связанных с хищением интеллектуальной собственности компаний. Нередко похищенная информация используется как гарант компенсации комфортного увольнения.

Для «подрабатывающих» и «внедренных» нарушителей цель определяет заказчик похищения информации, заставляя их как можно надежнее завуалировать свои действия. В зависимости от ситуации они могут прекратить зловредную для компании деятельность, имитировать производственную необходимость, а при особо неблагоприятных случаях пойти на взлом, подкуп коллег и иные меры, чтобы получить доступ к информации.

Результаты концептуального моделирования

Используя платформу имитационного моделирования Anylogic, визуализируем систему основных элементов поведения инсайдера и их взаимодействия применительно к двум случаям: когда он действует в одиночку, и когда ему помогают сообщники.

Первый случай. Исходя из статистических данных, типичными инсайдерами-одиночками выступают рядовые сотрудники, занимающие позицию программистов, инженеров, менеджеров и т. п. Как правило, их атаки являются технически простыми в исполнении, с использованием легальных прав и полномочий. Объектом атаки выступает все то, что, по мнению инсайдера, может иметь ценность для получения им в будущем тех или иных преимуществ (в том числе – предпринимательских: исходники программного обеспечения, производственные секреты, бизнес-планы, клиентские базы, бухгалтерские отчеты). Активная деятельность такого инсайдера продолжается от одного до трех месяцев. В этот период могут входить такие события, как принятие решения об увольнении, период преступной активности, заметание следов.

Для наглядности портрет одиночного внутреннего нарушителя и особенности его поведения при формировании угрозы кражи в системе информационной безопасности организации, развивая результаты работ [5; 6], представим в виде диаграммы причинно-следственных связей (рис. 2). На рисунке знаком плюс обозначены положительные связи, знаком минус – отрицательные, символом *L* – неоднозначные логические связи.

Рис. 2. Диаграмма причинно-следственных связей при формировании угрозы кражи информации со стороны одиночного инсайдера

Второй случай. В этом варианте картина причинно-следственных связей, в целом оставаясь похожей, учитывает взаимодействия с сообщниками при формировании умысла и самой кражи информации в организации (рис. 3).

Выводы

1. Инсайдерские угрозы, становясь все более значимой проблемой для самых различных компаний, требуют создания системного инструментария для своего анализа, прогнозирования и управления.

2. Для создания концептуальной модели инсайдерской деятельности необходимо:

– формализовать сложную систему информационного взаимодействия между участниками корпоративного процесса в компании, учитывающего предпринимательские, психологические, финансово-экономические и иные риски и мотивы;

– разработать стратегию информационной защиты, которая сочетает организационные и программно-технические средства и методы, включая системы предотвращения утечек данных (DLP-системы) [7; 8].

3. Одной из основных задач при построении системы информационной защиты компании является создание поведенческих моделей инсайдера-нарушителя на основе визуализации информации. В качестве метода визуализации поведения целесообразно использовать системно-динамические модели.

4. Перспективной платформой имитационного моделирования, с помощью которой может быть осуществлена визуализация системы основных элементов поведе-

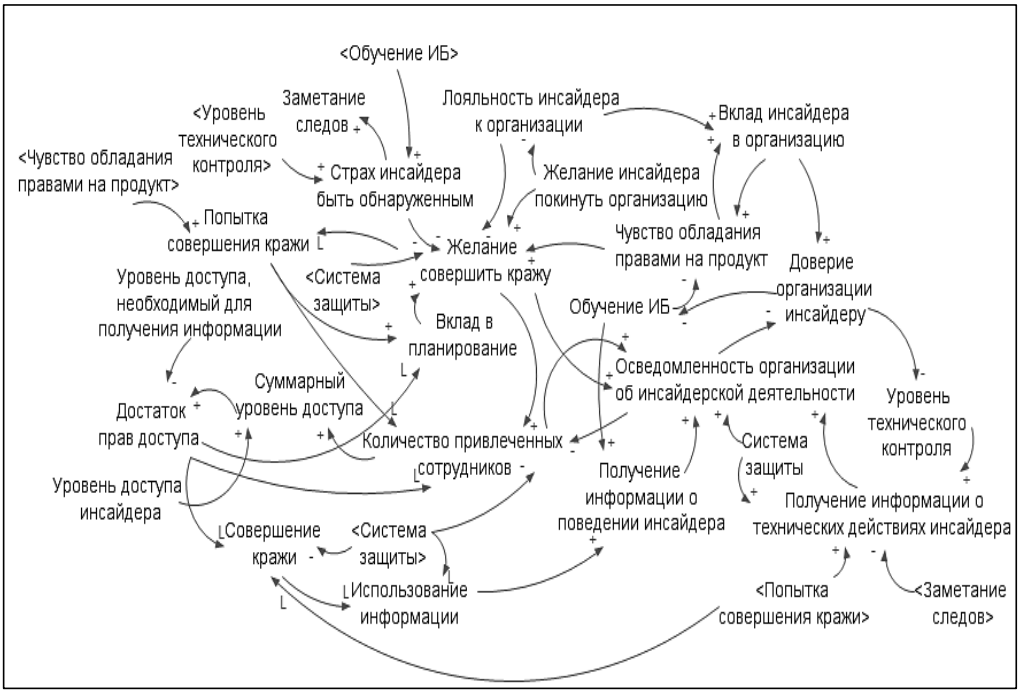

Рис. 3. Диаграмма причинно-следственных связей при формировании угрозы кражи информации со стороны инсайдера с соучастниками

ния инсайдера и их взаимодействия, является среда имитационного моделирования Anylogic.

5. С помощью Anylogic наглядно, компактно и логически четко представлены диаграммы причинно-следственных связей при формировании угрозы кражи информации со стороны инсайдера в одиночку и когда ему помогают сообщники.

6. Дальнейшее развитие концептуальных моделей связано с описанием зависимостей между элементами диаграмм на основе дифференциальных моделей, отражающих настройки системы защиты информации от внутреннего нарушителя, планирующего совершить кражу в одиночку или с соучастниками.

Литература

1. Инсайдерские угрозы в России 2009. – URL: http://www.perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_in_Russia_2009.pdf (дата обращения: 29.05.2018).

2. Утечки данных. – URL: https://www.infowatch.ru/analytics/ reports (дата обращения: 29.05.2018).

3. *Скворцов Н.А., Калиниченко Л.А., Ковалев Д.Ю.* Концептуальное моделирование предметных областей с интенсивным использованием данных // Тр. XVIII Международной конференции DAMDID/RCDL'2016 «Аналитика и управление данными в областях с интенсивным использованием данных», Ершово, 11–14 окт., 2016 г. – С. 7–15.

4. *Минаев В.А., Вайц Е.В., Грачева Ю.В*. Имитационные эксперименты с моделью информационно-психологических воздействий на массовое сознание // Безопасность информ. технологий. – 2017. – Т. 24. – № 2. – С. 61–71.

5. *Зайцев А.С., Малюк А.А*. Исследование проблемы внутреннего нарушителя // Вестн. РГГУ. – 2012. – № 14. – С. 114–134.

6. *Зайцев А.С., Малюк А.А.* Визуализация поведения внутреннего нарушителя информационной безопасности: кража интеллектуальной собственности // Вестн. РГГУ. – 2015. – № 12. – С. 76–91.

7. *Минаев В.А.* Простые числа: новый взгляд на закономерности формирования. – М. : Изд. дом «Логос Пресс», 2011. – 80 с.

8. Развитие методологических основ информатики и информационной безопасности систем / А.П. Фисун, А.Г. Касилов, В.Е. Фисенко, В.А. Минаев [и др.]. – М., 2004. – 253 с. – Деп. в ВИНИТИ, № 1165-В2004.

References

1. Insayderskie ugrozy v Rossii 2009. – URL: http://www.perimetrix.ru/downloads/rp/PTX_Insider_Security_Threats_in_Russia_2009.pdf (data obrashcheniya: 29.05.2018).

2. Utechki dannykh. – URL: https://www.infowatch.ru/analytics/ reports (data obrashcheniya: 29.05.2018).

3. *Skvortsov, N.A., Kalinichenko, L.A., Kovalev, D.Yu.* Kontseptual'noe modelirovanie predmetnykh oblastey s intensivnym ispol'zovaniem dannykh // Tr. XVIII Mezhdunarodnoy konferentsii DAMDID/RCDL'2016 "Analitika i upravlenie dannymi v oblastyakh s intensivnym ispol'zovaniem dannykh", Ershovo, 11–14 okt., 2016 g. – S. 7–15.

4. *Minaev, V.A., Vayts, E.V., Gracheva, Yu.V*. Imitatsionnye eksperimenty s model'yu informatsionno-psikhologicheskikh vozdeystviy na massovoe so-znanie // Bezopasnost' inform. tekhnologiy. – 2017. – T. 24. – № 2. – S. 61–71.

5. *Zaytsev, A.S., Malyuk, A.A*. Issledovanie problemy vnutrennego narushitelya // Vestn. RGGU. – 2012. – № 14. – S. 114–134.

6. *Zaytsev, A.S., Malyuk, A.A.* Vizualizatsiya povedeniya vnutrennego narushitelya informatsionnoy bezopasnosti: krazha intellektual'noy sobstvennosti // Vestn. RGGU. – 2015. – № 12. – S. 76–91.

7. *Minaev, V.A.* Prostye chisla: novyy vzglyad na zakonomernosti formirovaniya. – M. : Izd. dom "Logos Press", 2011. – 80 s.

8. Pazvitie metodologicheskikh osnov informatiki i informatsionnoy bezopasnosti sistem / A.P. Fisun, A.G. Kasilov, V.E. Fisenko, V.A. Minaev [i dr.]. – M., 2004. – 253 s. – Dep. v VINITI, № 1165-V2004.