УДК 519.87:004.891.3

РАЗРАБОТКА МЕТОДА ДИАГНОСТИКИ РИСКА ИНСАЙДЕРСКИХ УГРОЗ

Фадюшин С.Г.

[1]ФГАОУ ВО «Дальневосточный федеральный университет», Владивосток, e-mail: fadyushin.sg@dvfu.ru

Статистические данные свидетельствуют, что риск внутренних угроз для кибербезопасности предприятий находится на высоком уровне и продолжает расти. Отсюда следует, что необходимо разрабатывать и внедрять эффективные методы борьбы с подобными угрозами. Однако внутренние угрозы выявить непросто, т.к. инсайдер имеет законный доступ к конфиденциальной информации предприятия, знаком со структурой данных и, как правило, знает особенности системы защиты информации, что облегчает ему обход мер безопасности. Цель проведённого исследования заключается в теоретическом обосновании метода и соответствующего диагностического критерия оценки инсайдерской зависимости в поведении пользователя – сотрудника предприятия, имеющего доступ к конфиденциальной информации. Основным методом исследования служит метод вероятностной оценки смысла, разработанный автором. В результате проведенного исследования для оценки риска внутренних угроз предлагается использовать диагностический критерий инсайдерской зависимости в виде дифференциальной энтропии ключевых слов и выражений поисковых запросов пользователя в Сети по данным анализаторов контента. Результаты проведённого исследования могут быть полезны специалистам по информационной безопасности, исследователям психологии Интернета и разработчикам программного обеспечения, специализирующихся на технологиях выявления киберугроз.

Ключевые слова: внутренняя угроза, информационная безопасность, кибербезопасность, инсайдер, инсайдерская зависимость, информация, энтропия, аддикция

DEVELOPMENT OF A METHOD FOR DIAGNOSING THE RISK OF INSIDER THREATS

Fadyushin S.G.

FGAOU VO Far Eastern Federal University, Vladivostok, e-mail: fadyushin.sg@dvfu.ru

Statistical data indicate that the risk of internal threats to the cybersecurity of enterprises is at a high level and continues to grow. It follows that it is necessary to develop and implement effective methods to combat such threats. However, it is not easy to identify internal threats, because the insider has legitimate access to confidential information of the enterprise, is familiar with the data structure and, as a rule, knows the features of the information security system, which makes it easier for him to bypass security measures. The purpose of the study is to theoretically substantiate the method and the corresponding diagnostic criterion for assessing insider dependence in the behavior of a user – an employee of an enterprise with access to confidential information. The main method of research is the method of probabilistic assessment of meaning developed by the author. As a result of the conducted research, to assess the risk of internal threats, it is proposed to use the diagnostic criterion of insider dependence in the form of differential entropy of keywords and expressions of user search queries in the network according to content analyzers. The results of the study can be useful to information security specialists, Internet psychology researchers and software developers specializing in technologies for detecting cyber threats.

Keywords: internal threat, information security, cybersecurity, insider, insider addiction, information, entropy, addiction

Как правило, когда говорят о кибербезопасности, то имеют в виду различные внешние угрозы, исходящие от злоумышленников. При этом часто упускается из виду или в целях сохранения репутации предприятия, что угрозы для кибербезопасности исходят не только от внешних злоумышленников. К числу лиц, представляющих собой серьезный и растущий риск, также относятся халатные, небрежные, скомпрометированные и злонамеренные пользователи – инсайдеры. Внутренняя угроза (инсайдерская угроза) – это угроза информационной безопасности предприятия, в результате совершения которой различные конфиденциальные данные могут быть раскрыты и дискредитированы непосредственно сотрудниками предприятия, имеющими легитимный доступ к информационным системам, приложениям и базам данных. По определению Федеральной службы по техническому и экспортному контролю РФ, «инсайдер (Insider) – сотрудник предприятия, который причиняет или планирует причинение ущерба активам организации или помогает в такой акции внешнему нарушителю» [1].

Компании стараются не предавать огласке инциденты, исходящие от их внутренних пользователей (пользователей-сотрудников), но статистика свидельствует, что с каждым годом количество инцидентов с участием инсайдеров возрастает, и внутренние угрозы становятся наиболее опасными финансовыми рисками. Так, по статистическим данным, приведённым в [2], за последнее время затраты предприятий, связанные с внутренними угрозами, по все-

му миру увеличились до 15,38 млн долларов и в процентном выражении за последние три года составили: 2018 г. – 53%, 2020 г. – 60%, 2022 г. – 67%. Большинство (68%) организаций отмечают, что инсайдерские атаки за последнее время стали увеличиваться. При этом «инструментами» для инсайдеров служат: мессенджеры (33%), съёмные носители (25%), облачные хранилища, личная и корпоративная почта (8%). К основным мотивам инсайдеров относятся: финансовая или карьерная выгода, ущерб репутации предприятия.

По разным литературным источникам можно выделить следующие типы инсайдеров:

- недовольные (обиженные) сотрудники, у которых, например, может отсутствовать продвижение по карьерной лестнице, существуют внутренние конфликты;
- психически неустойчивые сотрудники, у которых злоупотребление конфиденциальными данными выражается в виде эмоциональной реакции на внешние стрессовые ситуации;
- вредоносные инсайдеры – сотрудники, которые совершают противоправные действия из побуждений злонамеренного характера;
- внутренние агенты – сотрудники, которые по сути являются шпионами внутри компании;
- халатные и небрежные сотрудники – сотрудники, которые способствуют совершению инсайдерских атак по ошибке или став жертвой фишинга.

Таким образом, приведённые статистические данные свидетельствуют о том, что риск внутренних угроз находится на высоком уровне и продолжает расти. Отсюда следует, что необходимо разрабатывать и внедрять эффективные методы борьбы с этими угрозами. Однако проблема в том, что внутренние угрозы выявить достаточно сложно, т.к. инсайдер имеет законный доступ к конфиденциальной информации предприятия, знаком со структурой данных и, как правило, осведомлён о системе защиты информации. Инсайдеры действуют тихо и незаметно, но при этом могут нанести серьёзный финансовый ущерб и навредить репутации предприятия.

Цель данного исследования заключается в обосновании метода и критерия диагностики риска инсайдерских угроз на основе принципов теории вероятностной оценки смысла. В основу исследования положен метод диагностики интернет-зависимого поведения человека, изложенный в статьях [3; 4]. Основные принципы теории вероятностной оценки смысла описаны в работе [5].

Материалы и методы исследования

Анализ статистических данных и сведений, полученных из литературных источников, показывает, что мотивы инсайдеров имеют, как правило, в основном психологический характер и часто сопровождаются стрессовым состоянием. К ним относятся: выгода, месть, саботаж, провоцирование изменений, самоудовлетворение, идеологические проявления, и просто наличие склонности к злонамеренным поступкам. Отмечается, что перед совершением атаки почти у всех инсайдеров изменялось поведение [6]. Если сотрудник выглядит недовольным, затаил обиду и с чрезмерным энтузиазмом выполняет больше задач сверх установленного норматива, то это может косвенно свидетельствовать о подготовке им инсайдерской атаки. Более подробно существующие классификации инсайдеров и их мотивации рассмотрены в [7].

Для борьбы с внутренними угрозами разрабатываются различные системы аналитики поведения пользователей (UBA и UEBA-системы). Например, в работе [8] предлагается эвристический алгоритм выявления аномалий в деятельности пользователей-сотрудников на основе модели БД NoSQL. К другим примерам можно отнести модели и алгоритмы обнаружения инсайдерских угроз, которые основаны на технологиях больших данных и машинного обучения [9]. Для защиты от внутренних угроз также необходимо совершенствовать организационную и нормативно-правовую базу, включая информирование сотрудников предприятия о ведении надзора за их деятельностью.

Таким образом, из приведённых данных и сведений можно сделать вывод, что психологический портрет инсайдера имеет схожие черты с психологическим портретом интернет-зависимого человека. Не случайно один из признаков инсайдерской угрозы заключается в частых запросах сотрудников на доступ к данным, которые не связаны с их должностными обязанностями. Близость психологических характеристик инсайдера и интернет-зависимого человека даёт основание говорить о проявлении у некоторых типов людей аддикции, которую можно было бы назвать инсайдерской зависимостью. Отсюда следует, что наблюдения за аномальной активностью пользователей-сотрудников на уровне компьютерной сети может помочь выявить внутренний риск, исходящий от них.

В исследованиях по психологии Интернета в качестве одной из объяснительных причин возникновения зависимости

от Интернета приводится связь между интернет-зависимостью и опытом потока – психическим состоянием, в котором человек полностью сосредоточен на том, чем он занимается [10; 11]. Состояние потока не ограничивается какой-либо одной сферой деятельности, а распространяется на всё, во что вовлечен человек. Как видно из определения, оба феномена психологически подобны, т.к. связаны с поведенческим повторением каких-либо действий, зависящих от внешних и внутренних психологических факторов, как и инсайдерская зависимость. Поэтому переживание опыта потока также может служить объяснительной причиной возникновения инсайдерской зависимости.

Человек с признаками инсайдерской зависимости, находясь в Сети, очевидно, чаще всего будет обращаться к какой-то одной заведомо определённой теме (повышение по службе, получение финансовой выгоды, наказание за преступную деятельность и т.п.). В этом случае набор слов его поисковых запросов (аномалия) по уровню осмысленности будет отличаться от уровня осмысленности среднестатистического набора слов поисковых запросов в состоянии нормы (норма). Сравнивая осмысленность текущих поисковых запросов с нормой, можно количественно оценить (диагностировать) вероятность риска инсайдерской угрозы, исходящей от зависимого сотрудника.

Уровень осмысленности набора слов поисковых запросов можно определить, используя принципы теории вероятностной оценки смысла. Согласно этой теории, механизм выработки человеком осмысленных умозаключений состоит в силлогизме Бейеса – Налимова [12]. В структуре силлогизма Бейеса – Налимова смысл описывается своей функцией распределения $p(\mu)$, мультипликативно взаимодействующей с фильтром $p(y/\mu)$. Взаимодействие описывается теоремой Бейеса и может быть представлено в виде формулы

$$p(\mu|y) = kp(y|\mu)\, p(\mu), \qquad (1)$$

где $p(\mu|y)$ – апостериорная условная функция распределения, описывающая семантику умозаключения; k – константа нормировки.

Формула Бейеса в виде (1), как показал В.В. Налимов, представляет собой силлогизм, т.е. имеются две посылки $p(\mu)$ и $p(y/\mu)$, из которых следует новая семантика $p(\mu/y)$, и в результате из отдельных семантических знаков (слов поисковых запросов) формируется программа осмысленных действий человека и соответствующая ей смысловая форма, такая как текст. Фильтр – это абстрактный элемент мышления, задающий условную функцию распределения $p(y/\mu)$.

Для иллюстрации единичного логического умозаключения в качестве примера ниже показана форма априорной функции распределения семантических знаков в виде отдельных слов (рис. 1).

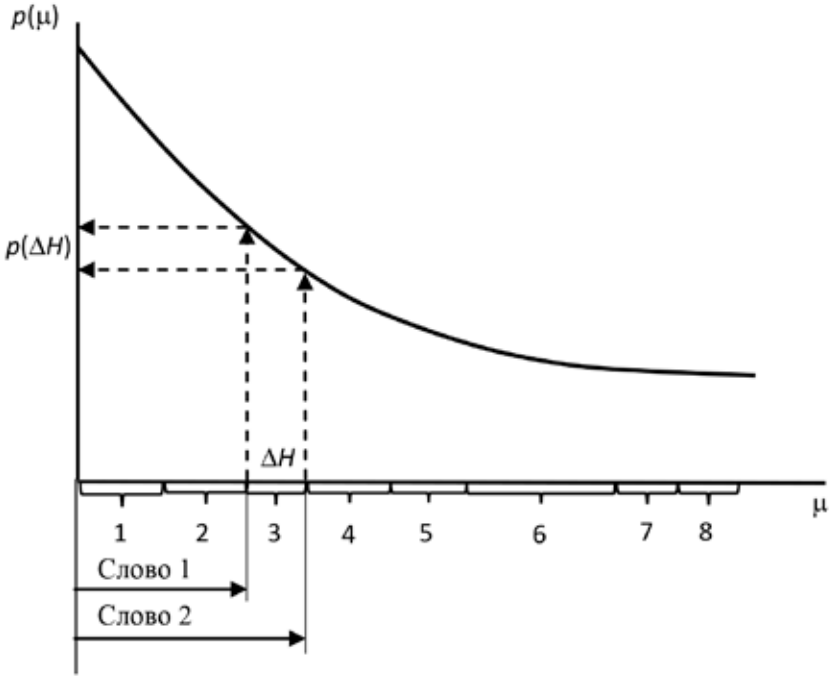

Рис. 1. Формирование логического умозаключения

Как видно на рис. 1, с каждым словом вероятностным образом связано множество смысловых значений. Ранги смысловых значений отложены по оси абсцисс μ и распределены по вероятности их появления $p(\mu)$, определяемой по оси ординат. Таким образом, каждому участку смысловой шкалы соответствуют свои вероятности, с которыми они ассоциируются со словом в сознании человека. Смысл, как это показано на рис. 1, заключен между словами. Тогда, если слова выразить в единицах информационной энтропии H, то отрезок между ними (в этом примере отрезок 3) покажет величину смысла – квант смысла ΔH:

$$\Delta H = |H(\text{Слово 1}) - H(\text{Слово 2})|.$$

Квант смысла представляет собой случайную величину. Тогда содержащий смысл код, состоящий из цепочки взаимосвязанных квантов смысла, можно охарактеризовать статистическими параметрами экспоненциального распределения непрерывной случайной величины. Формальным аналогом информационной энтропии для непрерывной случайной величины является дифференциальная энтропия, т.е. понятие смысла оказывается тождественным этому понятию, которое может служить мерой величины смысла M.

Исходя из описанных принципов теории вероятностной оценки смыслов, методика оценки инсайдерской зависимости будет заключаться в том, чтобы рассчитать, сравнить и проанализировать значения диагностических критериев M_i и M_a соответственно текущего и среднестатистического набора поисковых слов и фраз:

$M_i \geq M_a$ – риск инсайдерской угрозы маловероятен;

$M_i < M_a$ – есть вероятность, что у пользователя-сотрудника наблюдается тенденция к проявлению инсайдерской зависимости и, соответственно, есть риск внутренней угрозы.

Таким образом, уменьшение текущего уровня дифференциальной энтропии поисковых запросов отдельно взятого пользователя-сотрудника (M_i) по сравнению с его среднестатистическим уровнем дифференциальной энтропии поисковых запросов (M_a) в состоянии нормы может говорить о развитии у него инсайдерской зависимости и возникновении риска внутренней угрозы.

Результаты исследования и их обсуждение

Диаграммы функций плотности вероятности ΔH (разность информационных энтропий по Шеннону) для нормы и аномалии показаны на рис. 2 и 3 [3; 4].

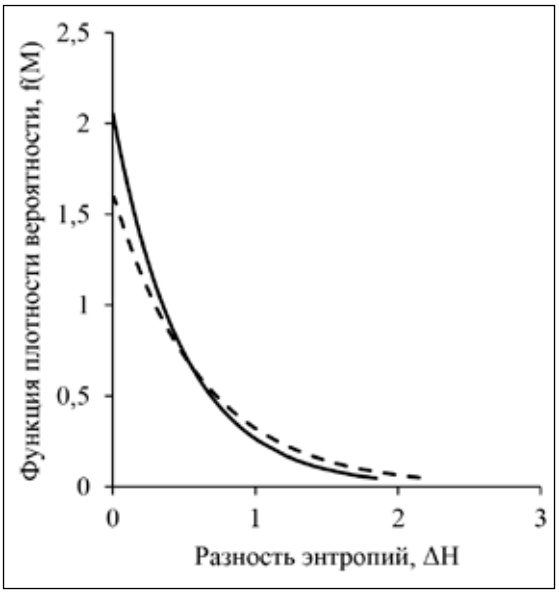

Рис. 2. Норма: сплошная линия – среднестатистический набор слов поисковых запросов; штриховая – текущий набор слов поисковых запросов

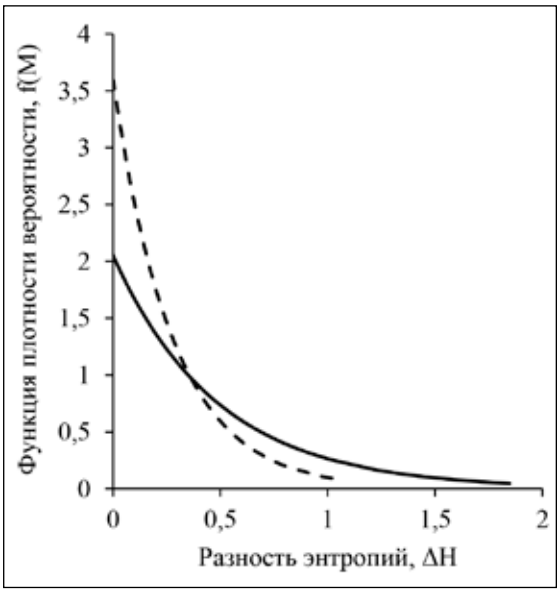

Рис. 3. Аномалия: сплошная линия – среднестатистический набор слов поисковых запросов; штриховая – текущий набор слов поисковых запросов

Анализ диаграмм, представленных на рис. 2 и 3, показывает, что при норме вероятность появления небольших по величине значений ΔH для набора слов текущих (повседневных) поисковых запросов пользователя-сотрудника будет меньше по сравнению с аномалией. Отсюда можно

сделать следующий вывод, что в состоянии инсайдерской зависимости пользователь-сотрудник, который сфокусировался на какой-то одной психологически важной для него проблеме, будет составлять поисковые запросы из однотипных, близких по значению слов. Эти слова будут отражать тот внутренний смысл (замысел), который осознанно или неосознанно будет пытаться реализовать зависимый человек.

В нормальном состоянии пользователь-сотрудник, не скованный довлеющей над ним психологической проблемой, может использовать разнообразные темы и слова для своих поисковых запросов, например такие, как работа, прибыль, отдых, новости, семья, образование и т.п. Для таких запросов требуются большие мыслительные усилия, свобода действий и творческий подход, соответственно, и уровень их осмысленности будет больше. В состоянии зависимости это невозможно. Слова-запросы и темы зависимого человека могут, например, быть такими: уголовное наказание, наказание, ответственность, уголовная ответственность и т.п.

Заключение

Предлагаемая в данной работе методика оценки риска инсайдерских угроз основана на вероятностной теории смыслов. Проявление инсайдерской активности у пользователя-сотрудника рассматривается как зависимость – инсайдерская зависимость, которая сопоставима с интернет-зависимостью. В качестве критерия диагностики инсайдерской зависимости предлагается использовать один из статистических параметров экспоненциального распределения непрерывной случайной величины – дифференциальную энтропию ключевых слов поисковых запросов пользователя-сотрудника в Сети. При снижении, особенно при немотивированном, текущего уровня дифференциальной энтропии поисковых запросов одного из сотрудников предприятия по сравнению со среднестатистическим уровнем дифференциальной энтропии поисковых запросов того же сотрудника может говорить о том, что у него формируется инсайдерская зависимость и, соответственно, риск возникновения внутренней угрозы повышается. Для получения более надёжного диагноза, действительно свидетельствующего о развитии у пользователя-сотрудника инсайдерской зависимости, рекомендуется дополнительно к разработанному методу использовать методы психодиагностики и соответствующее программное обеспечение.

Список литературы

1. Термины. [Электронный ресурс]. URL: https://bdu.fstec.ru/ubi/terms/terms/view/id/19 (дата обращения: 09.01.2023).

2. Руководство по внутренним угрозам. [Электронный ресурс]. URL: https://rt-solar.ru/upload/iblock/a0c/7foz1180v630bstsa6anybkfcsh5mxlo/Rukovodstvo-po-vnutrennim-ugrozam_vertikalnyy.pdf (дата обращения: 08.01.2023).

3. Fadyushin S.G., Vereshchagina E.A., Kayak A.B. Diagnosis of Internet-dependent Human Behavior in the Information Aspect. International Science and Technology Conference “FarEastCon” (ISCFEC 2019): Proceedings of the International Science and Technology Conference “FarEastCon” (ISCFEC 2019), Vladivostok, 01–04 October 2019 / Far Eastern Federal University. Vladivostok: Atlantis Press, 2019. P. 168-170. DOI: 10.2991/iscfec-19.2019.45.

4. Фадюшин С.Г. Интернет-зависимость как фактор аддиктивного поведения человека в киберпространстве // Современные наукоемкие технологии. 2020. № 2. С. 72-75. DOI: 10.17513/snt.37917.

5. Фадюшин С.Г. Вероятностная оценка смыслов. Логико-философский анализ проблемы смысла в кибернетике: монография. Владивосток: Издательство Дальневосточного федерального университета, 2022. 196 с.

6. Шугаев В.А., Алексеенко С.П. Классификация инсайдерских угроз информации // Вестник Воронежского института МВД России. 2020. № 2. С. 143-153.

7. Власов Д.С. К вопросу о мотивации инсайдера организации и способах его классификации // Научные труды КубГТУ. 2022. № 1. С. 128-147.

8. Котенко И.В., Ушаков И.А., Пелёвин Д.В., Преображенский А.И., Овраменко А.Ю. Выявление инсайдеров в корпоративной сети: подход на базе UBA и UEBA // Защита информации. Инсайд. 2019. № 5(89). С. 26-35.

9. Ушаков И.А., Котенко И.В., Овраменко А.Ю., Преображенский А.И., Пелёвин Д.В. Комбинированный подход к обнаружению инсайдеров в компьютерных сетях // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 4. С. 66-71. DOI: 10.46418/2079-8199_2020_4_10.

10. Войскунский А.Е. Вступительное слово // Психология. Журнал Высшей школы экономики. 2011. Т. 8. № 4. С. 29–34.

11. Войскунский А.Е. Психология и Интернет. М.: Акрополь, 2010. 439 с.

12. Fadyushin S.G., Vereshchagina E.A., Pafnuteva Y.V. Nalimov’s Bayesian Syllogism to Overcome the Barrier of Meaning in AI Systems. 2020 International Multi-Conference on Industrial Engineering and Modern Technologies, FarEastCon 2020, Vladivostok, 06–09 October 2020. Vladivostok, 2020. P. 9271411. DOI: 10.1109/FarEastCon50210.2020.9271411.