Разработка нечеткого классификатора входящих заявок на предоставление доступа пользователей к информационной инфраструктуре

Ю.В. Беликов

Ростовский государственный экономический университет (РИНХ)

Аннотация: В настоящее время одним из наиболее обширных вопросов в сфере информационной безопасности является организация разграничения доступа пользователе к объектам информационной инфраструктуры. С учётом объёмов корпоративных информационных ресурсов, а также количества пользователей, запрашивающих доступ, возникает необходимость автоматизации процесса согласования доступа с учетом возможных рисков. В данном случае наиболее оптимальным решением данной задачи является применение аппарата нечеткой логики. В статье проведён анализ процесса предоставления доступа к информационной инфраструктуре с помощью нечеткого классификатора и разработана концептуальная модель алгоритма нечеткого классификатора входящих заявок на предоставление доступа с целью автоматизации процесса и минимизации рисков информационной безопасности, связанных с возможными деструктивными действиями, нацеленными на конфиденциальность, целостность и доступность информационной инфраструктуры.
Ключевые слова: информационная безопасность, информационная инфраструктура, нечеткая логика, предоставление (разграничение) доступа, классификатор входящих заявок, средства защиты информации, ключевые показатели (критерии) оценки доступа.

Введение

На сегодняшней день трудно переоценить значение процесса обеспечения информационной безопасности в любых сферах бизнеса и экономики. Так, в своём исследовании, специалисты компании Positive Technologies указывают, что только за первые три квартала 2023 года количество выявленных целевых компьютерных атак выросло на 76% по сравнению с количеством атак, проведённых за весь 2022 год.

Одним из векторов кибератак является поиск учетных записей пользователей, имеющих привилегированные или избыточные права, с последующей попыткой компрометации учетных данных [1]. Результатами таких атак в большинстве случаев становятся: хищение чувствительной (конфиденциальной) информации, воздействие на бизнес-процессы компаний путём нарушения доступности сервисов, искажение

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

обрабатываемой информации. Также стоит отметить и работу внутреннего нарушителя информационной безопасности [1, 2]. В настоящее время наряду с хакерскими атаками активно развивается направление промышленного шпионажа и предумышленной утечки чувствительной информации, такой, как коммерческая тайна и персональные данные. Предпосылкой к таким действиям, в том числе, является получение злоумышленником «расширенных» прав доступа к информационным ресурсам, вызванное ошибкой в процессе согласования или вследствие сговора со специалистами, обрабатывающими поток входящих заявок на предоставление доступа [3].

Не смотря на стремительно изменяющейся ландшафт киберугроз, ежедневное выявление специалистами уязвимостей в программном коде, а также неумышленные и (или) умышленные действия пользователей, влекущие за собой компьютерные инциденты, компании всё более активно применяют средства защиты информации разных классов [4]. К таким средствам можно отнести:

- системы управления событиями информационной безопасности (SIEM);
- системы управления уязвимостями (VM);
- современные средства межсетевого экранирования (NGFW, UTM) с функциями обнаружения и предотвращения атак (IPS/IDS);
- антивирусные средства защиты;
- системы предотвращения утечки информации (DLP);
- системы контроля привилегированных учетных записей (PAM);
- системы управления учётными записями и администрирование (IDM/IGA).

Наиболее важным направлением в обеспечении конфиденциальности, целостности и доступности информации и информационных активов является превентивная защита данных, при котором «плоскость» атаки

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

значительно уменьшается путём применения специальных программно-аппаратных комплексов, а также мер по минимизированию пользовательских привилегий, контролю прав и доступов [5]. К таким мерам можно отнести процедуру предоставления доступа субъектам к объектам информационной инфраструктуры. На практике данная операция сводится к формальному согласованию заявки, оформленной в соответствующем порядке в системе электронного документооборота, системе Service Desk или соответствующей IDM/IGA-системах.

Опрос специалистов по информационной безопасности крупных ИТ-компаний показал, что на структурное подразделение по кибербезопасности, состоящее в среднем из 3 - 5 сотрудников, приходится порядка 300 - 400 заявок в день на согласование предоставления (изменения) доступа к ИТ-сервисам, что в соответствии со внутренними регламентами организации доступа занимает 60% - 70% рабочего времени. При этом большая часть времени отводится на ручную проверку легитимности запрашиваемого доступа, правильность оформления заявки и выполнение пользователем ряда установленных требований по обеспечению безопасной работы с запрашиваемым сервисом. Также, помимо согласования доступа, на специалистов возлагаются задачи по аудиту прав доступа пользователей к инфраструктуре, разработка (модернизация) моделей доступа, своевременная блокировка доступа субъектов к объектам и прочие задачи, связанные с организацией доступа к информационным активам [6].

Одной из важнейших задач является разработка эффективной системы анализа поступающего потока заявок с применением аппарата нечеткой логики, которая позволит максимально автоматизировать процесс согласования заявок на доступ к объектам информационной инфраструктуры.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

Анализ литературы показывает, что аппарат нечеткой логики активно применяется в таких сферах информационной безопасности, как оценка рисков наступления негативных событий в результате реализации уязвимостей или наступления событий, способных повлечь за собой нарушение конфиденциальности, целостности и доступности информации [7], анализ аномалий в информационной инфраструктуре, оценка выбора средств защиты, качественная оценка параметров работы сервисов [8]. Одним из инструментов решения задач информационной безопасности является экспертный метод, который представляет собой классическую качественную оценку рассматриваемого вопроса. Однако, внедрение результатов экспертной оценки в информационную инфраструктуру как качественных показателей не всегда представляется возможным и в данном случае нечеткая логика позволяет с высокой степенью точности интерпретировать качественную экспертную оценку в количественную [9].

Основными направлениями в изучении вопроса предоставления доступа в отечественной и зарубежной научной литературе являются вопросы обеспечения технически безопасного доступа к информационной инфраструктуре и правовое соответствие предоставления доступа к защищаемой информации. Тема применения нечеткой логики в процессе согласования доступа субъектов к объектам информационной инфраструктуры не описана в мере, достаточной для реализации программных механизмов, в том числе, взаимодействующих с IDM/IGA системами, способных автоматизировать процесс согласования заявок на предоставления доступа и минимизировать участие специалистов по информационной безопасности в этом процессе.

Формирование требований к процессу согласования доступа

Анализируя различные методы разграничения доступа к информационным системам, стоит отметить, что наиболее подходящими

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

являются классическая дискреционная и ролевая модели разграничения доступа. Выбор же конкретной модели зависит от ряда факторов, таких, как техническая возможность реализации той или иной модели и организационные требования со стороны владельцев сервиса. Но в основе обеих моделей лежит принцип соответствия запрашиваемого уровня доступа субъекта к объекту [10].

В классическом понимании процесс предоставления доступа представляет собой формализованную процедуру последовательного согласования заявки, составленной инициатором и адресованной владельцу сервиса. Концептуально процесс согласования доступа можно изложить следующим образом:

1. Заявитель (пользователь) в соответствии с установленными внутренними требованиями по информационной безопасности оформляет заявку на предоставление доступа к необходимым информационным ресурсам. В качестве дополнительной меры возможно добавление документа, подтверждающего, что пользователь ознакомлен с требованиями по информационной безопасности и с мерой ответственности за нарушение указанных требований.
2. После составления заявка попадает на согласование к непосредственному руководителю заявителя.
3. В случае согласования заявка поступает на рассмотрение специалистам по информационной безопасности.
4. Последним этапом является согласование заявки с владельцем объекта информационной инфраструктуры.

На каждом из этапов согласования специалистами проводится качественная оценка соответствия запрашиваемых прав на доступ требованиям локальных нормативных актов по информационной безопасности, а также правильность составления и оформления самой заявки.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

Стоит отметить, что на каждом из этапов (п. 2 – 4) согласующий может отправить на доработку или вовсе отклонить заявку, тем самым увеличивая количество циклов согласования.

Разработка нечеткого классификатора

Говоря математическим языком, для разработки нечеткого классификатора входящих заявок необходимо проработать следующие этапы классического механизма нечеткой логики (рисунок 1):

1) привести к нечеткости входящие данные;
2) разработать базу правил для работы с нечетким выводом;
3) описать процедуру нечеткого логического вывода;
4) провести оценку корректности процедуры приведения к четкому выводу.

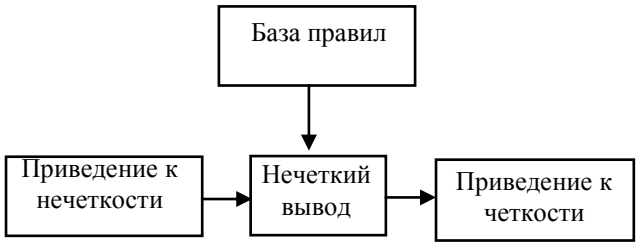

Рис. 1. – Этапы разработки нечеткого классификатора

На первом этапе необходимо рассмотреть этапы согласования как входящие данные. Важнейшим этапом согласования доступа субъектов к объектам информационной инфраструктуры является определение критериев, при которых уровень риска наступления негативного события (инцидента информационной безопасности) будет минимальным. С математической точки зрения происходит процесс определения универсальных множеств. Данные критерии являются результатом экспертной оценки и могут отличаться в зависимости от особенностей информационных (автоматизированных) систем и ландшафта

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

информационной инфраструктуры в целом. К таким критериям можно отнести:

1) соответствие запрашиваемой роли;
2) соответствие дискреционным правилам разграничения доступа;
3) наличие ошибок в оформлении заявки.

Ещё одним важным аспектом в организации процесса предоставления доступа является определение уровня критичности указанных выше требований или, в контексте аппарата нечетких множеств, лингвистические термы. Наиболее оптимальной в данном случае является трёхуровневая система качественной оценки уровня критичности, выражаемая, как:

- «Низкий уровень риска» – уровень, при котором возможно автоматическое согласование доступа без дополнительного анализа со стороны специалиста по информационной безопасности или привлечения дополнительных согласующих.

- «Средний уровень риска» – уровень, при котором возможно согласование доступа только после анализа такой заявки со стороны специалиста по информационной безопасности.

- «Высокий уровень риска» – уровень, при котором заявка будет автоматически отклонена.

Следующим этапом, необходимым для создания нечеткого классификатора, является сопоставление событий, способствующих наступлению инцидента информационной безопасности, и выбранных уровней риска.

С точки зрения примененные аппарата нечетких множеств, данная задача имеет следующий вид: имеются множество термов $L = \{l_1, l_2, \dots, l_m\}$ и универсальное множество $U = \{u_1, u_2, \dots, u_n\}$. Нечеткое множество $\tilde{l}_j$,

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

которым описывается лингвистический терм $l_j, \text{где } j = \overline{1,m}$, на универсальном множестве U представляется в виде следующей формулы (1):

$$\widetilde{l_j} = \left(\frac{\mu_{l_j}(u_1)}{u_1}, \frac{\mu_{l_j}(u_2)}{u_2}, \dots, \frac{\mu_{l_j}(u_n)}{n}\right), \quad (1)$$

где $\mu_{l_j}(u_i)$ – степень принадлежности нечеткому множеству.

Далее необходимо определить степени принадлежностей U к элементам множества L. В качестве примера воспользуемся методом статистической обработки экспертной информации. Данный метод базируется на статистическом анализе мнений группы экспертов. Будем считать, что экспертные оценки по данному вопросу бинарные (0, 1), т.е. 1 указывает на наличие у рассматриваемого элемента u_1 нечеткого множества $\widetilde{l_j}$, а 0 – на отсутствие. Информацию, полученную этим способом от экспертов, можно представить в виде таблицы № 1.

Таблица № 1

Общий вид опросника

	u_1	u_2	…	u_n
$\widetilde{l_1}$				
$\widetilde{l_2}$				
…				
$\widetilde{l_n}$				

Для решения задачи необходимо вычислить степень принадлежности нечеткому множеству рассчитывается по следующей формуле (2):

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

$$\mu_{l_j}(u_i) = \frac{1}{E}\sum_{e=\overline{1,E}} o_{j,i}^{e}, \text{ при } i = \overline{1,n}, \quad (2)$$

где E – количество экспертов, $o_{j,i}^{e}$ – мнение e-го эксперта о наличии у элемента u_i свойств нечеткого множества $\tilde{l}_j$.

Смоделируем результат опроса экспертов учитывая бинарную модель оценки (таблица №2).

Таблица № 2

Результат опроса

Эксперты (E)	**Термы (L)**	**Универсальное множество (U)**		
		несоответствие запрашиваемой роли	**несоответствие дискреционным правилам**	**наличие ошибок в оформлении**
Эксперт 1	Низкий уровень риска	0	0	1
	Средний уровень риска	0	0	0
	Высокий уровень риска	1	1	0
Эксперт 2	Низкий уровень риска	0	0	1
	Средний уровень риска	1	0	0
	Высокий уровень риска	0	1	0
Эксперт 3	Низкий уровень риска	0	0	1
	Средний уровень риска	0	1	0

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

Эксперты (E)	**Термы (L)**	**Универсальное множество (U)**		
		несоответствие запрашиваемой роли	**несоответствие дискреционным правилам**	**наличие ошибок в оформлении**
	Высокий уровень риска	1	0	0
Эксперт 4	Низкий уровень риска	0	0	0
	Средний уровень риска	0	0	1
	Высокий уровень риска	1	1	0
Эксперт 5	Низкий уровень риска	0	0	1
	Средний уровень риска	0	0	0
	Высокий уровень риска	1	1	0

Результат обработки экспертных оценок в соответствии с формулой принадлежности нечеткому множеству представлен в таблице №3. В каждой строке таблицы представлено два численных значения: первый (верхний) – общее количество голосов, отданных за принадлежность нечеткому множеству; второй (нижний) – степень принадлежности.

Исходя из таблицы №3, следует, что по мнению экспертов наиболее высокий уровень риска наступления инцидента информационной безопасности связан с согласованием заявок, в которых явно прослеживается несоответствие запрашиваемой роли доступа или указаны избыточные дискреционные права. Наличие же ошибок в оформлении заявки в меньшей

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

степени может повлиять на конфиденциальность, целостность или доступность информационных активов или обрабатываемой информации.

Таблица № 3

Результат обработки мнений экспертов.

Термы (L)	**Универсальное множество (U)**		
	несоответствие запрашиваемой роли	**несоответствие дискреционным правилам**	**наличие ошибок в оформлении**
Низкий уровень риска	0	0	4
	0	0	0,8
Средний уровень риска	1	1	1
	0,2	0,2	0,2
Высокий уровень риска	4	4	0
	0,8	0,8	0

Заключение

В ходе исследования был проведён анализ основных тенденций информационной безопасности в сфере предоставления доступа пользователям к информационным ресурсам. Статистические данные об объёме поступающих заявок на согласование доступа указывают на актуальность рассматриваемой темы и на необходимость автоматизации этого процесса. В статье описаны основные принципы согласования доступа к ресурсам с помощью классификатора входящих заявок с использованием метода статистической обработки экспертной информации.

Литература

1. Сахно В.В., Маршаков Д.В., Айдинян А.Р. Применение методов нечеткой логики для решения задачи обеспечения информационной безопасности // Молодой исследователь Дона. 2018. №4 (13). URL:

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

cyberleninka.ru/article/n/primenenie-metodov-nechetkoy-logiki-dlya-resheniya-zadachi-obespecheniya-informatsionnoy-bezopasnosti.

2. Любухин А.С. Методы анализа рисков информационной безопасности: нечеткая логика // International Journal of Open Information Technologies. 2023. №2. URL: cyberleninka.ru/article/n/metody-analiza-riskov-informatsionnoy-bezopasnosti-nechetkaya-logika.

3. Борисов В.В., Гончаров М.М. Модель выбора мероприятий по обеспечению информационной безопасности на основе нечетких автоматов // Программные продукты и системы. 2014. №1 (105). URL: cyberleninka.ru/article/n/model-vybora-meropriyatiy-po-obespecheniyu-informatsionnoy-bezopasnosti-na-osnove-nechetkih-avtomatov.

4. Mynuddin Mohammed, Hossain Iqbal Mohammad, Khan Uddin Sultan, Islam Anwarul Mohammad. Cyber Security System Using Fuzzy Logic // Conference: 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). URL: researchgate.net/publication/374137561_Cyber_Security_System_Using_Fuzzy_Logic

5. Картак В.М., Гатиятуллин Т.Р. Методика анализа рисков информационной безопасности в банковской сфере с использованием нечеткой логики // Проблемы науки. 2018. №2 (26). URL: cyberleninka.ru/article/n/metodika-analiza-riskov-informatsionnoy-bezopasnosti-v-bankovskoy-sfere-s-ispolzovaniem-nechetkoy-logiki.

6. Жукова М.Н., Коромыслов Н.А. Модель оценки защищенности автоматизированной системы с применением аппарата нечеткой логики // Известия ЮФУ. Технические науки. 2013. №12 (149). URL: cyberleninka.ru/article/n/model-otsenki-zaschischennosti-avtomatizirovannoy-sistemy-s-primeneniem-apparata-nechetkoy-logiki.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

7. Хохлов Н.С., Канавин С.В., Рыбокитов А.Е. Логико-лингвистическая нечеткая модель для оценки рисков нарушения информационной безопасности в самоорганизующихся сетях связи и управление ими // Вестник ВИ МВД России. 2019. №2. URL: cyberleninka.ru/article/n/logiko-lingvisticheskaya-nechetkaya-model-dlya-otsenki-riskov-narusheniya-informatsionnoy-bezopasnosti-v-samoorganizuyuschihsya

8. Астахова Л.В., Цимбол В.И. Применение самообучающейся системы корреляции событий информационной безопасности на основе нечеткой логики при автоматизации систем менеджмента информационной безопасности // Вестник ЮУрГУ. Серия: Компьютерные технологии, управление, радиоэлектроника. 2016. №1. URL: cyberleninka.ru/article/n/primenenie-samoobuchayuscheysya-sistemy-korrelyatsii-sobytiy-informatsionnoy-bezopasnosti-na-osnove-nechetkoy-logiki-pri.

9. Заводцев И.В., Гайнов А.Е., Ржевский Д.А. Интеллектуальные системы управления инцидентами информационной безопасности // Перспективы развития информационных технологий. 2015. №24. URL: cyberleninka.ru/article/n/intellektualnye-sistemy-upravleniya-intsidentami-informatsionnoy-bezopasnosti.

10. Бопп В.А. Типы моделей разграничения доступа // Известия ТулГУ. Технические науки. 2020. №5. URL: cyberleninka.ru/article/n/tipy-modeley-razgranicheniya-dostupa.

References

1. Sahno V.V., Marshakov D.V., Ajdinjan A.R. Molodoj issledovatel' Dona. 2018. №4 (13). URL: cyberleninka.ru/article/n/primenenie-metodov-nechetkoy-logiki-dlya-resheniya-zadachi-obespecheniya-informatsionnoy-bezopasnosti.

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

2. Ljubuhin A.S. International Journal of Open Information Technologies. 2023. №2. URL: cyberleninka.ru/article/n/metody-analiza-riskov-informatsionnoy-bezopasnosti-nechetkaya-logika.

3. Borisov V. V., Goncharov M. M. Programmnye produkty i sistemy. 2014. №1 (105). URL: cyberleninka.ru/article/n/model-vybora-meropriyatiy-po-obespecheniyu-informatsionnoy-bezopasnosti-na-osnove-nechetkih-avtomatov.

4. Mynuddin Mohammed, Hossain Iqbal Mohammad, Khan Uddin Sultan, Islam Anwarul Mohammad. Conference: 2023 3rd International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME). URL: researchgate.net/publication/374137561_Cyber_Security_System_Using_Fuzzy_Logic.

5. Kartak V.M., Gatijatullin T.R. Problemy nauki. 2018. №2 (26). URL: cyberleninka.ru/article/n/metodika-analiza-riskov-informatsionnoy-bezopasnosti-v-bankovskoy-sfere-s-ispolzovaniem-nechetkoy-logiki.

6. Zhukova M.N., Koromyslov N.A. Izvestija JuFU. Tehnicheskie nauki. 2013. №12 (149). URL: cyberleninka.ru/article/n/model-otsenki-zaschischennosti-avtomatizirovannoy-sistemy-s-primeneniem-apparata-nechetkoy-logiki.

7. Hohlov N.S., Kanavin S.V., Rybokitov A.E. Vestnik VI MVD Rossii. 2019. №2. URL: cyberleninka.ru/article/n/logiko-lingvisticheskaya-nechetkaya-model-dlya-otsenki-riskov-narusheniya-informatsionnoy-bezopasnosti-v-samoorganizuyuschihsya.

8. Astahova L.V., Cimbol V.I. Vestnik JuUrGU. Serija: Komp'juternye tehnologii, upravlenie, radiojelektronika. 2016. №1. URL: cyberleninka.ru/article/n/primenenie-samoobuchayuscheysya-sistemy-korrelyatsii-sobytiy-informatsionnoy-bezopasnosti-na-osnove-nechetkoy-logiki-pri.

9. Zavodcev I.V., Gajnov A.E., Rzhevskij D.A. Perspektivy razvitija informacionnyh tehnologij. 2015. №24. URL:

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024

cyberleninka.ru/article/n/intellektualnye-sistemy-upravleniya-intsidentami-informatsionnoy-bezopasnosti.

10. Bopp V.A. Izvestija TulGU. Tehnicheskie nauki. 2020. №5. URL: cyberleninka.ru/article/n/tipy-modeley-razgranicheniya-dostupa.

Дата поступления: 28.06.2024

Дата публикации: 17.08.2024

© Электронный научный журнал «Инженерный вестник Дона», 2007–2024