Инженерный вестник Дона, №8 (2022)
ivdon.ru/ru/magazine/archive/n8y2022/7868

Применение экспертных данных при построении регрессионной модели оценки уровня защищенности носителей информации

С.И. Носков, А.А. Бутин

Иркутский государственный университет путей сообщения

Аннотация: Представлен обзор публикаций российских и зарубежных исследователей по вопросам моделирования процесса оценки степени защищённости отдельных компонент объекта информатизации (автоматизированной системы). Проанализированы основные факторы, влияющие на уровень защищенности. Приведены типы объектов несанкционированного воздействия. Обоснованы выбор в качестве основного обобщённого объекта «носитель информации» и списка актуальных угроз для него, проведён их краткий анализ. В качестве выходной (зависимой) переменной разрабатываемой регрессионной модели определен уровень защищенности носителей информации. Входными (независимыми) переменными являются степени опасности угроз: неправомерного ознакомления с защищаемой информацией; несанкционированного копирования защищаемой информации; преодоления физической защиты; утраты носителей информации. Разработанная модель имеет вид регрессионного уравнения и может применяться при прогнозировании уровня защищенности носителей информации.
Ключевые слова: информационная безопасность; объект информатизации; автоматизированная система; носители информации; угрозы информационной безопасности; уровень защищённости; регрессионная модель; экспертная информация; критерии адекватности.

Введение

Анализ уровня защищенности носителей информации (НИ) является весьма актуальным в сфере информационной безопасности. В настоящее время эта проблема успешно решается, в том числе, и с применением методов математического моделирования. Так, в работе [1] предлагается метод оценки защищенности киберфизических систем, основанный на классификаторе угроз, что позволяет оценить текущий уровень защищенности и дать рекомендации по выделению ограниченных ресурсов защиты на основе экспертной оценки известных угроз. Такой подход позволяет выполнять динамическое моделирование объекта в автономном режиме, своевременно определять возможности злоумышленников и формировать превентивные меры защиты на основе анализа угроз. При моделировании могут использоваться актуальные базы оценки реальных угроз и инцидентов в киберфизических системах, что позволяет проводить

экспертную оценку их влияния как на службы безопасности, так и на отдельные ее компоненты. В [2] процессы в системах машинного обучения рассматриваются с учетом возможных вредоносных воздействий. Представлены результаты моделирования событий, приводящих к нарушению безопасности систем машинного обучения, работающих на объектах критической информационной инфраструктуры. С целью исследования сценариев перехода систем машинного обучения в опасное состояние и численной оценки вероятности нарушения безопасности было проведено математическое моделирование угроз логико-вероятностным методом. Работа [3] посвящена оценке пяти наиболее часто используемых операционных систем Microsoft Windows, Apple Mac и Linux на предмет обнаруженных уязвимостей и риска, связанного с каждой из них. Описана статистическая методология и лежащий в ее основе математический подход. В статье [4] анализируется проблема кибербезопасности компьютерных сетей управления электроснабжением на уровне железных дорог и предлагается граф топологии компьютерной сети управления электропотреблением.

Обоснование выбора переменных модели

Как известно, информация нематериальна, но хранится на материальных носителях. Следовательно, в целях сохранения её в безопасном состоянии с точки зрения классических критериев (конфиденциальность, целостность, доступность (КЦД)) для НИ следует обеспечить необходимый (адекватный) уровень защищённости. Кроме этого, согласно общепринятым методикам эшелонированная защита информации должна обеспечиваться в том числе на отдельном выделенном уровне НИ от угроз различного вида.

Также очевидно, что в условиях высокой степени неопределённости функционирования автоматизированной системы (АС) большое значение приобретают различные технологии адекватного экспертного оценивания уровня защищённости того или иного компонента информационной инфраструктуры. При этом применение технологии использования экспертных данных (ЭД) в том числе предполагает использование экспертом различных методологических инструментов оценки защищённости объекта воздействия (ОВ) (см., например, [5-7]).

Далее отметим, что Федеральная служба по техническому и экспортному контролю (ФСТЭК) России имеет достаточно полный Банк данных угроз [8]. Исходя из этого, в целях демонстрации описываемой в данной статье методики используется обобщённый ОВ «носители информации», где очевидно находится та информация, КЦД которой необходимо защищать.

Для определённости с целью описания метода оценки уровня защищённости НИ выделим следующие наиболее актуальные угрозы (условно) из данного Банка данных ФСТЭК:

1. Угроза неправомерного ознакомления с защищаемой информацией;
2. Угроза несанкционированного копирования защищаемой информации;
3. Угроза преодоления физической защиты;
4. Угроза утраты носителей информации.

Приведем краткий анализ данных угроз.

Угроза 1 состоит в возможности реализации несанкционированного доступа к информации на НИ с использованием не только штатных, но и добавочных/наложенных программно-аппаратных средств.

При реализации угрозы 2 (У2) появляется возможность полного доступа к защищаемым данным (хранящимся на НИ), поскольку механизм разграничения, реализованный в штатной ОС (приложении), после

получения копии информации на съёмный носитель (или в другое место, доступное нарушителю вне системы), уже не функционирует. У2 обусловлена уязвимостями механизмов разграничения доступа к защищаемой информации на НИ и/или контроля доступа лиц в контролируемой зоне, а также возможна при отсутствии защиты криптографическими средствами.

Реализация угрозы 3 (У3) состоит в преодолении нарушителем механизмов системы управления и контроля доступа (СКУД) в защищаемые помещения организации, в которых находятся аппаратные средства АС (включая НИ). Очевидным образом У3 обусловлена недостаточностью мер в реализации СКУД: ошибками персонала; отсутствием видеонаблюдения и/или охранной сигнализации и другими уязвимостями в системе инженерно-физической защиты.

Реализация угрозы 4 обусловлена недостаточностью мер по обеспечению защищённости от нарушения конфиденциальности и доступности информации при утрате (в том числе хищении) НИ: халатность сотрудников; хранение информации на НИ в незашифрованном виде; отсутствие актуальной копии (как следствие, нарушения регламента резервного копирования данных); недостатки в системе учёта НИ и т.д.

Построение регрессионной модели оценки уровня защищенности носителей информации на основе экспертных данных

Введем необходимые обозначения:

y – уровень защищенности носителей информации (в %);

x_i – степень опасности i-ой угрозы, $i=\overline{1,4}$, при этом:

x_1 – угроза неправомерного ознакомления с защищаемой информацией;

x_2 – угроза несанкционированного копирования защищаемой информации;

x_3 – угроза преодоления физической защиты;

x_4 – угроза утраты носителей информации.

Регрессионную модель, связывающую зависимую переменную y и независимые переменные x_i, $i=\overline{1,4}$, будем строить в линейной форме

$$y_k=\alpha_0+\sum_{i=1}^{4}\alpha_i x_{ki}, \quad k=\overline{1,n}, \qquad (1)$$

где α_i, $i=\overline{1,4}$ – подлежащие оцениванию параметры, k – номер наблюдения, n – длина выборки данных.

При построении модели (1) воспользуемся подходом, предложенным в работах [9, 10]. Вначале с помощью датчика случайных чисел зададим элементы матрицы наблюдений независимых переменных $X=\|x_{ki}\|$, $k=\overline{1,20}$, $i=\overline{1,4}$, где $x_{ki}\in(0,1)$. При этом $n=20$. Затем организуем процедуру формирования группой из трех опытных в области защиты информации экспертов векторов наблюдений зависимой переменной y^i, $i=\overline{1,3}$,каждый из которых, по мнению эксперта, должен соответствовать матрице X. Естественно, при этом $y_k^i\in(0,100)$, $k=\overline{1,20}$, $i=\overline{1,3}$. Заметим, что эксперты формируют свою информацию независимо друг от друга. Сформированная таким образом исходная информация приведена в таблице.

Таблица. Исходная информация

y^1	y^2	y^3	y^4	x_1	x_2	x_3	x_4
1	2	3	4	5	6	7	8
55	52	50	52.58	0.30	0.18	0.50	0.22
15	13	10	13.02	0.87	0.83	0.77	0.62
56	53	50	53.36	0.30	0.14	0.75	0.20
39	43	40	40.98	0.64	0.68	0.43	0.33
30	32	35	31.98	0.82	0.50	0.55	0.35
30	27	30	28.68	0.72	0.60	0.64	0.41
20	23	20	21.32	0.82	0.57	0.62	0.48
44	41	45	42.90	0.62	0.73	0.29	0.27
35	30	35	32.80	0.73	0.54	0.52	0.69
51	48	45	48.36	0.53	0.52	0.42	0.34

1	2	3	4	5	6	7	8
50	47	45	47.58	0.50	0.32	0.62	0.51
45	50	55	49.40	0.51	0.24	0.35	0.50
40	43	40	41.32	0.38	0.73	0.26	0.55
40	37	35	37.58	0.83	0.36	0.40	0.43
78	85	80	81.52	0.09	0.08	0.12	0.31
34	37	40	36.64	0.66	0.74	0.37	0.67
42	45	50	45.08	0.64	0.91	0.50	0.39
18	20	15	18.22	0.50	0.40	0.90	0.66
24	21	20	21.80	0.54	0.65	0.79	0.77
50	55	60	54.40	0.38	0.34	0.48	0.60

Построим три регрессионных модели вида (1) по информации каждого эксперта, используя обычный метод наименьших квадратов.

а). Модель с наблюдаемым вектором значений зависимой переменной y^1.

$$y=91.75-31.98x_1-14.33\ x_2-30.69\ x_3\ -23.16x_4, \qquad (2)$$

$$R^1=0.88,\ F^1=27.4, E^1=12.4.$$

Здесь R^1 – критерий множественной детерминации, F^1- критерий Фишера, E^1 – средняя относительная ошибка аппроксимации (в%).

б). Модель с наблюдаемым вектором значений зависимой переменной y^2.

$$y=95.89-36.43x_1\ -13.56x_2\ -38.40x_3\ -18.28x_4, \qquad (3)$$

$$R^2=0.90,\ F^2=35.3,\ E^2=9.8.$$

в). Модель с наблюдаемым вектором значений зависимой переменной y^3.

$$y=93.88-30.90x_1\ -12.83x_2\ -44.64x_3\ -14.84x_4, \qquad (4)$$

$$R^3=0.83,\ F^3=18.4,\ E^3=15.3.$$

Как следует из анализа моделей (2) – (4), та из них, которая построена на основе информации второго эксперта, наиболее точна. При этом все три модели обладают вполне приемлемыми значениями используемых критериев адекватности.

Далее, в соответствии с предложенным в [9] алгоритмом, сформируем вектор y^4 по правилу:

$$y^4=\sum_{i=1}^{3}\omega_i y^i,\ \omega_i>0,\ \sum_i^3\omega_i=1, \qquad (5)$$

где ω_i – весовые коэффициенты линейной свертки (5), каждый из которых тем больше, чем более точна модель, построенная по информации соответствующего эксперта. Примем в качестве меры точности критерий Фишера. Тогда указанные коэффициенты следует определять по формуле:

$$\omega_i=F^i/\sum_{j=1}^{3}F^j.$$

В результате получим: ω_1=0.34, ω_2=0.44, ω_3=0.22, после чего компоненты вектора y^4, вычисленные по формуле (5), станут равны числам, размещенным в табл.1.

Построим модель (1) на основе информации, соответствующей вектору y^4:

$$y=94.04-33.70x_1-13.66x_2-37.15x_3-19.18x_4, \qquad (6)$$

$$R^4=0.89,\ F^4=31.5,\ E^4=10.2.$$

Модель (6) и следует считать полученной по всей совокупности экспертной информации. Она является вполне адекватной и может быть успешно использована как для анализа характера влияния независимых переменных x_i, $i=\overline{1,4}$ на выходной фактор y, так и для прогнозирования значений последнего.

Заключение

В работе приведена и обоснована методика построения регрессионной модели оценки уровня защищённости носителей информации в случае применения экспертных данных. При этом, в качестве факторов, влияющих на степень защиты, использованы угрозы из перечня ФСТЭК России. Технология построения модели может быть использована в практической деятельности при проведении процедур аудита информационной безопасности АС организации.

Литература

1.Yevseiev S., Pohasii S., Milevskyi S., Fedorenko R., KurchenkoO.Development Of A Method For Assessing The Security Of Cyber-Physical Systems Based On The Lotkavolterra Model //Eastern-European Journal of Enterprise Technologies. 2021. №5. P. 30-47.

2.Chekmarev M.A., Klyuev S.G., Shadskiy V.V. Modeling security violation processes in machine learning systems// Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2021. 21(4). P. 592-598.

3.Hitigala Kaluarachchilage P.K., Attanayake C., Rajasooriya S., TsokosC.P. An analytical approach to assess and compare the vulnerability risk of operating systems// International Journal of Computer Network and Information Security. 2020. 12(2). P. 1-10.

4.Stasiuk O.I., Grishchuk R.V., GoncharovaL.L. Mathematical. Differential Models and Methods for Assessing the Cybersecurity of Intelligent Computer Networks for Control of Technological Processes of Railway Power Supply//Cybernetics and Systems Analysis. 2018. 54(4). P. 671-677.

5. Носков С.И., Бутин А.А. Методическое обеспечение оценки уровня уязвимости объектов информатизации // Информационные технологии и проблемы математического моделирования сложных систем. 2015. № 14. С. 38-48.

6. Петрова О.В., Поздняков А.А., Уваров А.В. Риск пребывания автоматизированной информационной системы специального назначения в критическом состоянии // Инженерный вестник Дона. 2021. № 11. URL: ivdon.ru/ru/magazine/archive/n11y2021/7284.

7. Куликова О.В., Пиневич Е.В., Домбаян Г.С., Егоров Н.В., Волохов А.С. Оценка защищенности информации при передаче данных между субъектами

доступа в клиент-серверной архитектуре // Инженерный вестник Дона. 2021. № 4. URL: ivdon.ru/ru/magazine/archive/n4y2021/6900.

8. Банк данных угроз безопасности информации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» // URL: bdu.fstec.ru/threat?size=50/ (дата обращения: 20.07.2022).

9. Носков С.И., Торопов В.Д. Формирование исходной информации и идентификация параметров экспертной модели статистического типа // Современные технологии. Системный анализ. Моделирование. 2004. №4. С.103-106.

10. Бутин А.А., Носков С.И., Торопов В.Д. Спецификация статистической модели деятельности предприятия малого бизнеса // Информационные технологии и проблемы математического моделирования сложных систем. 2006. № 4. С. 59-63.

References

1. Yevseiev S., Pohasii S., Milevskyi S., Fedorenko R., Kurchenko O. Eastern-European Journal of Enterprise Technologies. 2021. №5. pp. 30-47.

2. Chekmarev M.A., Klyuev S.G., Shadskiy V.V. Scientific and Technical Journal of Information Technologies, Mechanics and Optics. 2021. 21(4). pp. 592-598.

3. Hitigala Kaluarachchilage P.K., Attanayake C., Rajasooriya S., Tsokos C.P. International Journal of Computer Network and Information Security. 2020. 12(2). pp. 1-10.

4. Stasiuk O.I., Grishchuk R.V., GoncharovaL.L.Mathematical. Cybernetics and Systems Analysis. 2018. 54(4). pp. 671-677.

5. Noskov S.I., Butin A.A. Informacionnie tehnologii i problemi matematicheskogo modelirovayij slozgnih system. 2015. №. 14. pp. 38-48.

6. Petrova O.V., Pozdnijkov A.A., Uvarov A.V. Inzhenernyj vestnik Dona. 2021. №. 11. URL:ivdon.ru/ru/magazine/archive/n11y2021/7284.

7. Kulikova O.V., Pnevich E.V., Dombaijn G.S., Egorov N.V., Volohov A.S. Inzhenernyj vestnik Dona. 2021. №. 4. URL: ivdon.ru/ru/magazine/archive/n4y2021/6900.

8. Bank dannih ugroz bezopasnosti informacii FAU «GNII PTZI FSTEK Rossii» [Data Bank of Information Security Threats of the State Research Institute of PtZI of the Federal Service for Technical and Export Control of the Russian Federation]. URL:bdu.fstec.ru/threat?size=50 (accessed 12/07/2022).

9. Noskov S.I., Toropov V.D. Sovremennie tehnologii. Sistemnii analiz. Modekirovanie. 2004. №. 4. pp.103-106.

10. Butin A.A., Noskov S.I., Toropov V.D. Informacionnye tehnologii i problemy matematicheskogo modelirovania slozgnih system. 2006. №. 4. pp. 59-63.