Для цитирования: Лачихина А. Б., Петраков А. А. Целостность данных как критерий оценки защищенности ресурсов корпоративных информационных систем // Вопросы радиоэлектроники. 2019. № 11. С. 77–81.
DOI 10.21778/2218-5453-2019-11-77-81
УДК 658.382.3

А. Б. Лачихина[1], А. А. Петраков[2]

[1] Московский государственный технический университет им. Н. Э. Баумана, Калужский филиал,
[2] АО «НПП «КПЗ «Тайфун»

ЦЕЛОСТНОСТЬ ДАННЫХ КАК КРИТЕРИЙ ОЦЕНКИ ЗАЩИЩЕННОСТИ РЕСУРСОВ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

Рассмотрен вопрос оценки защищенности информационных ресурсов при управлении информационной безопасностью на промышленном предприятии. Приведены основные аспекты обеспечения информационной безопасности как процесса. В качестве критерия оценки защищенности ресурсов корпоративной информационной системы предложено использовать целостность данных, определяемую как вероятность возможного нарушения целостности в соответствующем процессе переработки информации. Рассмотрены группы технологических операций, относящихся к процессу переработки информации. Приведен набор вероятностей возможных событий, которые способствуют поддержанию целостности данных. Для математической постановки задачи каждое из событий рассмотрено как альтернатива с заданным критерием оптимизации. Введение целевой функции для множества альтернатив позволяет выбрать наилучшую из них и установить причину нарушения целостности. Отмечается зависимость полной вероятности нарушения целостности от априорного распределения вероятностей.

Ключевые слова: *информационная безопасность, информационный ресурс, вероятность нарушения целостности данных*

Введение

Одним из необходимых компонентов управления современным промышленным предприятием является корпоративная информационная система (КИС). Информация – ресурс, необходимый для функционирования предприятия, а информационная система – инструментарий для ее хранения, передачи и обработки.

Характерными чертами современных КИС являются постоянно увеличивающиеся объемы информационных ресурсов и потоков данных, циркулирующих внутри системы, высокие требования к качественным характеристикам инфраструктуры, глубокое сплетение с методиками управления предприятием несколькими или многими группами пользователей, имеющими разные права. Как следствие, информационные системы для оперирования данными используют не только технологию баз данных, но и хранилища данных с механизмами статистического анализа и многомерным представлением независимо от архитектуры самой КИС [1].

Одним из наиболее важных свойств информационной системы предприятия является безопасность ее информационных ресурсов. Исторически сферой защиты информации являлось противодействие намеренному нарушению ее конфиденциальности, то есть несанкционированному копированию, прочтению, замене, уничтожению и т. п. Основными инструментами при этом были шифрование, перекрытие каналов утечки информации и контроль доступа к информационной инфраструктуре. Последние 10–15 лет чаще стал употребляться термин «информационная безопасность» (ИБ), благодаря которому появилось понимание, что достаточно большой ущерб информационным активам могут нанести не только несанкционированный доступ или преднамеренные вредоносные воздействия.

Защита информационной системы должна обеспечивать защищенность информационных ресурсов от любых умышленных или случайных угроз с помощью различных средств: программных, аппаратных и т. д. При этом необходимо учитывать, что в состав КИС входит программное, аппаратное, техническое обеспечение, персонал (оперативный и эксплуатационный) и сами данные. Соответственно, периметр безопасности должен охватывать все элементы системы.

Большинство мероприятий по защите информации возлагается на систему обеспечения ИБ – совокупность нормативных, организационных, технических, аппаратных, языковых и программных средств, предназначенных для организации,

поддержания и контролирования защищенности данных в КИС, а также процессов их переработки. Кроме того, на предприятии целесообразно создавать систему управления ИБ, являющуюся одним из аспектов управления предприятием в целом. В российском стандарте ГОСТ ИСО/МЭК 27001–2006 вводится понятие «Система менеджмента информационной безопасности». Она представляет собой часть общей системы менеджмента, в основе которой лежат методы, позволяющие оценить бизнес, – риски при проектировании, внедрении, функционировании, мониторинге, анализе, улучшении и поддержке ИБ [2]. Как отмечено в стандарте, подобные системы должны объединять организационные структуры, политику, деятельность при планировании, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы [2].

Таким образом, необходимым этапом управления ИБ КИС является оценка информационных рисков для ее активов с применением количественных или качественных методик. Под оценкой риска понимается регулярная обработка информации с целью определения источников риска, количественного определения его величины и сравнения полученного показателя с заданными критериями риска [2]. Результаты используются для определения методов реакции предприятия на существующий уровень ИБ, пересмотра политики безопасности или подтверждения эффективности применяемых средств ее обеспечения.

Целостность данных в качестве критерия оценки защищенности информационных ресурсов

На данный момент наиболее распространенным критерием оценки степени защищенности как при внешнем, так и при внутреннем аудите безопасности информационной системы является показатель информационного риска. Однако далеко не всегда есть необходимость или возможность проводить полную количественную оценку рисков ИБ в условиях функционирования производства.

В качестве более простого критерия оценки защищенности информационных ресурсов КИС может быть использована целостность данных, которая является одним из трех взаимозависимых компонентов комплексного понятия ИБ [3, 4]. Целостность данных предлагается оценивать вероятностью возможного нарушения целостности в соответствующем процессе обработки информации.

Задача определения названных вероятностей должна решаться для конкретной информационной системы, так как каждая из них обладает уникальным набором программного, аппаратного и технического обеспечения, к числу которых также относятся средства обеспечения ИБ. В соответствии с процессным подходом к менеджменту ИБ имеет смысл рассматривать работу КИС как набор процессов, в частности обработки, хранения, передачи. А решение задачи определения вероятностей потребует алгоритмического описания данных процессов.

На рисунке представлены процессы переработки информационных потоков при обработке запросов пользователей в информационной системе предприятия, соотнесенные с уровнями сетевой модели OSI.

Для каждого процесса переработки информации требуется определить следующие вероятности:

- при выполнении функциональной задачи – вероятность надежного представления информации;
- вероятность представления требуемой информации за заданное время;
- в базах данных – вероятность того, что полностью отражены реальные объекты учета конкретного типа;
- в проверяемой информации – вероятность отсутствия скрытых случайных ошибок;
- вероятность того, что не возникнет скрытых случайных ошибок со стороны пользователей или обслуживающего персонала ИС до или за время выполнения задачи;
- вероятность того, что не произойдет скрытого вирусного воздействия и выполнение задачи не прервется антивирусной профилактикой до или за время выполнения задачи;
- вероятность сохранения актуальности информации на момент ее использования;
- вероятность предотвращения несанкционированного доступа;
- вероятность того, что не произойдет аппаратного или программного сбоя до или за время выполнения задачи;
- вероятность сохранения целостности данных.

Случайное событие, описываемое этими вероятностями, рассмотрим как некоторую альтернативу x_i из множества X, позволяющих сохранить целостность данных. Может быть задана функция $z(x)$ для всех $x_i \in X$, названная критерием (или параметром) оптимизации, которая обладает следующим свойством: если $x_2 > x_1$, то $z(x_2) > z(x_1)$. Если целевая функция $Z = f(x) \Rightarrow \max$ или $\min$, то для всего множества $X = \{x_1, x_2, ..., x_n\}$ любая выбранная альтернатива приведет к однозначно известным последствиям (сохранению целостности данных), а заданный критерий $z(x)$ численно выражает оценку этих последствий. Альтернатива, которая обладает наибольшим значением критерия, является наилучшей [5]:

$$x^* = \arg\max z(x) \text{ при } x \in X. \quad (1)$$

Рисунок. Информационные потоки при обслуживании запросов клиентов

Задача нахождения оптимального решения x^* зависит от того, является ли множество X конечным, счетным или континуальным, а также является ли критерий функцией или функционалом.

Трудность задачи нахождения наилучшей альтернативы на практике значительно возрастает [6], что связано с ее многокритериальностью. Тогда несколько критериальных функций $Z_i = f_i(x)$, где $i = 1, n$, нужно свернуть в унитарный обобщенный численный признак – суперкритерий, скалярную функцию векторного аргумента

$$Z_0 = Z_0(f_i(x)), \text{ где } i = 1, n. \quad (2)$$

Используем аддитивные

$$Z_0 = \sum_{i=1}^{n} \frac{p_i f_i(x)}{a_i} \quad (3)$$

или мультипликативные функции

$$Z_0 = \prod_{i=1}^{n} \frac{f_i(x)^{p_i}}{a_i}, \quad (4)$$

где a_i – значение, обеспечивающее упорядочение разнородных критериев; p_i – вес, определяющий вклад частного критерия в суперкритерий

$$p_i \in (0, 1], \sum_{i=1}^{n} p_i = 1. \quad (5)$$

Веса начальных показателей в интегральном индексе зависят от их дисперсий и корреляции между ними.

Если перерабатываемый информационный ресурс (сообщение) является дискретной случайной величиной, то характеристика целостности есть вероятность трансформации истинного значения сообщения x_i в некоторое другое x_j, $i \neq j$. Это будет условной вероятностью $p_{ij} = p(x_j/x_i)$.

Полная вероятность нарушения целостности $P_{\text{нц}}$ зависит от априорного распределения вероятностей на ансамбле возможных сообщений

$$P_{\text{нц}} = \sum_{i=1}^{m} p(x_i)\, p(x_j / x_i). \quad (6)$$

Выводы

В работе установлено, что полная вероятность нарушения целостности данных зависит от априорного распределения вероятностей трансформации истинных значений информационных ресурсов в процессе обработки информации. Таким образом, можно сделать вывод, что целостность данных наряду с информационными рисками может применяться в качестве критерия оценки защищенности информационных ресурсов промышленного предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Лачихина А.Б. Управление безопасностью систем баз данных // Вопросы радиоэлектроники. 2017. № 6. С. 50–54.
2. ГОСТ Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2019. 31 с.
3. ГОСТ Р ИСО/МЭК 15408-1-2002. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. М.: ИПК Издательство стандартов, 2002. 35 с.
4. Постаутов М.Е., Осипов Д.Л. Модель многоуровневой защиты целостности данных в приложениях баз данных // Сборник материалов V Всероссийской научно-технической конференции «Студенческая наука для развития информационного общества». 2016. С. 447–450.
5. Костогрызов А.И. Математические модели процессов функционирования информационных систем. Ч. 1 // КомпьюЛог. 1999. № 1. С. 39–44.
6. Подиновский В.В. Согласительные решения многокритериальных задач выбора // Проблемы управления. 2017. № 2. С. 17–26.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Лачихина Анастасия Борисовна, к.т.н., доцент, Калужский филиал ФГБОУ ВО «Московский государственный технический университет имени Н.Э. Баумана (Национальный исследовательский университет)», Российская Федерация, 248000, Калуга, ул. Баженова, д.2, тел.: 8 (4842) 22-48-84, e-mail: anastaisalach73@gmail.com.

Петраков Андрей Алексеевич, генеральный директор, АО «НПП Калужский приборостроительный завод «Тайфун», Российская Федерация, 248009, Калуга, Грабцевское ш., д.174, тел.: 8 (4842) 71-85-85, e-mail: info@typhoon-jsc.ru.

For citation: Lachikhina A.B., Petrakov A.A. Data integrity as a criterion for assessing the security of corporate information systems resources. Voprosy radioelektroniki, 2019, no. 11, pp. 77–81.
DOI 10.21778/2218-5453-2019-11-77-81

A.B. Lachikhina, A.A. Petrakov

DATA INTEGRITY AS A CRITERION FOR ASSESSING THE SECURITY OF CORPORATE INFORMATION SYSTEMS RESOURCES

The paper considers the information resources protection assessing in the information security management in an industrial enterprise. The main aspects of information security as a process are given. It is proposed to use data integrity as a criterion for resources security assessing of the corporate information system, defined as the probability of a possible violation of the integrity in the corresponding process of processing information. The groups of technological operations related to the process of information processing are considered. An approximate set of probabilities of possible events that contribute to maintaining data integrity is given. For the mathematical formulation of the problem, each of the events is considered as an alternative with a given optimization criterion. The introduction of a target function for a variety of alternatives allows you to select the best one and determine the cause of the integrity violation. The dependence of the total probability of integrity violation on a priori probability distribution is noted.

Keywords: information security, information resource, probability of data integrity violation

REFERENCES

1. Lachikhina A.B. Database security management. *Voprosy radioelektroniki,* 2017, no. 6, pp. 50–54. (In Russian).
2. GOST R ISO/MEK 27001–2006. *Information technology. Security techniques. Information security management systems. Requirements.* Moscow, Standartinform Publ., 2019, 31 p. (In Russian).
3. GOST R ISO/MEK 15408-1-2002. *Information technology. Security techniques. Evaluation criteria for IT security. Part 1. Introduction and general model.* Moscow, Izdatelstvo standartov Publ., 2002, 35 p. (In Russian).
4. Postautov M.E., Osipov D.L. Multilevel data integrity protection model in database applications. (Conference proceedings) 5th Vserossiiskaya nauchno-tekhnicheskaya konferentsiya «Studencheskaya nauka dlya razvitiya informatsionnogo obshchestva», 2016, pp. 447–450. (In Russian).
5. Kostogryzov A.I. Mathematical models of the processes of functioning of information systems. Pt. 1. *CompuLog,* 1999, no. 1, pp. 39–44. (In Russian).
6. Podinovskiy V.V. Conciliation decisions of multicriteria selection problems. *Problemy upravleniya,* 2017, no. 2, pp. 17–26. (In Russian).

AUTHORS

Lachikhina Anastasiya, Ph. D., associate professor, Bauman Moscow State Technical University (Kaluga Branch), 2, Bazhenova St., Kaluga, 248000, Russian Federation, tel.: +7 (4842) 22-48-84, e-mail: anastasialach73@gmail.com.
Petrakov Andrey, general director, NPP Kaluga instrument-making plant TYPHOON JSC, 174, Grabtsevskoye road, Kaluga, 248009, Russian Federation, tel.: +7 (4842) 71-85-85, e-mail: info@typhoon-jsc.ru.