DOI: 10.18137/RNU.V9187.23.01.P.20 УДК 004.852

М.А. Золотухина, С.В. Зыков

ИССЛЕДОВАНИЕ И ОПРЕДЕЛЕНИЕ ПРИЗНАКОВ СКРЫТЫХ АТАК НА ПРЕДПРИЯТИИ ДЛЯ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ[1]

Аннотация. Зачастую именно человеческий фактор ведет к распространению угроз на предприятиях. Если техническое устройство представляет собой четко работающий и слаженный механизм с возможностью при помощи диагностического оборудования проводить замеры параметров неисправностей и устранять их, то для исследования скрытых атак необходим новый компонент системы. Предприятия и промышленность в целом нуждаются в интеллектуальной системе защиты и обнаружения скрытых угроз на основе алгоритмов машинного обучения. Для обнаружения скрытых угроз требуется комплекс мер по установлению признаков, анализу всех составляющих компонентов, возможности осуществления процесса прогнозирования с высокой точностью и вынесения рекомендаций.
Рассматриваются проблемы создания базы знаний исторических данных уязвимостей на предприятиях. Проведено исследование перенасыщения признаками диагностической информации и приведены предостережения при переобучении нейросети. Показаны методы обработки данных и применение их на практике. Исследование статистики обнаружения атак и уязвимостей на предприятиях и анализ человеческого фактора с исторической точки зрения входит в структуры проявления скрытых угроз. Это является одним из главных критериев идентификации уязвимостей. Все рассмотренные методы, результаты, представленные в статье, являются подходящим слоем для реорганизации данных в знания и применимы для следующих исследований. Если учитывать историю компании по определенным критериям и на этом этапе осуществлять интеллектуальный анализ диагностических данных, то нужно обратить внимание на составляющие значений. Именно наличие признаков идентификации, указанных в статье, позволяет с высокой точностью выявлять неблагоприятные события в информационных системах предприятия. Возникают задачи прикладного характера, связанные с необходимостью усовершенствования анализа внутренних и внешних параметров объекта исследования с целью обнаружения скрытых угроз.

Ключевые слова: обработка данных, защита данных, большие данные, интеллектуальный анализ данных, машинное обучение.

M.A. Zolotukhina, S.V. Zykov

INVESTIGATION AND IDENTIFICATION OF SIGNS OF HIDDEN ATTACKS IN THE ENTERPRISE FOR MACHINE LEARNING ALGORITHMS

Abstract. Common attack styles imply human exploitation, namely cyber attacks, unskilled workers, staff negligence, unhealthy workplace environment. The spread of threats in enterprises often creates a human factor. If the technical device is a well-functioning and well-coordinated mechanism, which enables to measure the parameters of malfunctions and eliminate them using the diagnostic equipment, then a new system component is needed to investigate hidden attacks. Enterprises and industry as a whole need an intelligent system of protection and detection of hidden threats based on machine learning algorithms. To detect hidden threats, a set of measures is required to identify signs, analyze all components, predict and make recommendations, which is shown in the sections.

[1] Выражаем благодарность Российскому технологическому университету – МИРЭА за предоставленную возможность проводить исследования в области искусственных нейронных сетей, защиты данных и программной инженерии.

Золотухина Мария Александровна
аспирант, МИРЭА – Российский технологический университет, Москва. Сфера научных интересов: искусственные нейронные сети; машинное обучение; защита данных; управление в информационных системах; интеллектуальный анализ данных. Автор более 10 опубликованных научных работ. ORCID: 0000-0001-9819-7435.
Электронный адрес: rtu_mary@mail.ru

Зыков Сергей Викторович
доктор технических наук, доцент, МИРЭА – Российский технологический университет, Москва; профессор департамента программной инженерии, НИУ «Высшая школа экономики», Москва. Сфера научных интересов: корпоративные информационные системы; IT-кризисология; разработка гетерогенных систем; технология семантической интеграции данных. Автор более 120 опубликованных научных работ. SPIN-код: 4149-8264.
Электронный адрес: szykov@hse.ru

The article discusses the problems of creating a knowledge base of historical vulnerability data at enterprises. A study of the oversaturation of diagnostic information with signs and retraining of the neural network was also conducted. Studies of data processing methods and their application in practice are shown. The study of the statistics of the detection of attacks and vulnerabilities at enterprises and the analysis of the human factor from a historical point of view is included in the structures of the manifestation of hidden threats. This is one of the main criteria for identifying vulnerabilities. All the methods considered, the results of which can be seen in the article, are a suitable layer for reorganizing data into knowledge and are applicable in the following studies. There are applied problems associated with the need to improve the analysis of internal and external parameters of the object of study in order to detect hidden threats.

Keywords: data processing, data protection, big data, data mining, machine learning.

Введение

Анализ исторических данных подразумевает непрерывную интеллектуальную обработку параметров больших объемов данных [1]. Такие меры применяются для выявления наиболее слабых сторон производства, стратегии, экономической составляющей компании [2]. Накопленные технические характеристики изделий, хронология событий, выполненная техническими специалистами, журналы эксплуатации – всё это считается историческими данными. Данные классифицируются датчиками регистрации и измерительными устройствами. Но в зависимости от направления производства компании часто отказываются от сбора данных, так как не имеют облачных технологий и отдельных подразделений, занимающихся внедрением инновационных разработок в области BigData, следовательно, у них нет возможности хранить и обрабатывать большие массивы диагностической информации. Для создания рекомендательной системы требуется выделить качественные и количественные признаки в диагностической информации. Составление правил предполагает использование данных в хронологическом порядке.

Организации, квалифицирующиеся на разработке программных средств для защиты данных, предоставляют услуги либо локально, либо облачно используют машинное обучение и технологии BigData. Также есть корпорации, главные направления которых тесно

связаны с обработкой данных, например, провайдеры цифровых услуг и сервисов. Предприятия, занимающиеся торговлей, начиная от переработки вторсырья и заканчивая продажей гвоздей, не сконцентрированы на внедрении анализа данных для определения параметров, которые в полной мере классифицировали бы спрос на продукты и услуги, определяли недостатки работы организации, осуществляли дополнительный сбор данных для определения пожеланий потенциальных клиентов. Всё ориентировано на интуицию. Но нельзя не упомянуть о полномасштабных проектах компаний, где всё зависит от изучения и оценки процессов.

Далее рассмотрим методы обработки и анализа для диагностики на примере информационных систем промышленных предприятий и корпораций [3].

Постановка проблемы

В большинстве случаев предприятия не ведут никаких записей. Данная ситуация, возможно, связана с организацией работы в структурах предприятия. Для качественного анализа нужны пространственные данные, то есть общая диагностическая информация о внутренней среде объектов исследования. Чтобы разрабатываемый метод прогнозирования выдавал качественный результат, следует подобрать такие данные, главные аспекты уязвимостей которых смогут быть описаны точными признаками. Эта потребность осложняется отсутствием этих данных. Кроме того, не вся диагностическая информация является подходящей, прежде всего – узкопрофильная экспертная оценка состояний [4].

Самые распространенные проблемы в наборах исторических данных заключаются в отсутствующих значениях, то есть неопределенных ячейках параметров, а также нетипичных данных, а именно выбросов, неинформативных данных-дубликатов и несогласованных данных, представленных в разных регистрах или форматах.

Чтобы алгоритмы прогнозирования выдавали качественный результат, нужно предварительно провести очистку и реорганизацию диагностических параметров [5]. Для создания и поддержания функционала прогнозной модели потребуются исторические данные, собранные в равные промежутки времени, обработка признакового пространства и применение интеллектуального анализа [6].

Цели исследования

Чтобы решить задачу отсутствия диагностической информации, требуется применить методы очистки данных. Использование методов математической статистки позволит осуществить дополнение пропусков критериев в датасете, тем самым выстроить пропорциональную зависимость столбцов и строк. Коэффициент корреляции позволит восстановить числовые параметры и создать оптимальное решение. Восстановление недостающих данных дает возможность использовать среду признакового пространства эффективно.

Исследование характеристик аналитическим программным обеспечением влияет на процесс обучения нейронной сети. Данный способ с меньшей вероятностью переносит увеличение ошибочных решений с выходящего слоя персептрона. Также рассмотрение вопроса о взаимосвязи данных разных категорий позволяет не пренебрегать остаточными значениями и сфокусироваться на процессе обучения. Следовательно, главная цель рассмотрения исторической информации – создание датасета с параметрами пространственных данных объекта исследования. Чтобы определить параметры скрытых угроз на предприятии, потребуется большая производительность алгоритмов [7]. Для этого параллельно вводятся дополнительные средства обработки данных и интеллектуального анализа.

В компаниях обнаружение угроз останавливается на взаимодействии с внешними консультантами и созданием внутреннего контроля. Анализ данных в условиях преднамеренных и умышленных атак, поиск скрытых угроз и использование прогностической системы не предусмотрены, так как в компаниях зачастую нет даже отдела безопасности в области обнаружения уязвимостей.

Для определения главной тематики признаков вернемся на стадию анализа предприятий и их уязвимостей. Классификация характеристик по сведениям о скрытых атаках анализируется на основе алгоритма кластеризации. Такой подход дает возможность вычислить большое количество связей между компонентами уязвимостей. Полученные статистические данные анализируются в таких системах, как Yandex Cloud Marketplace. Таким образом можно получить линейные диаграммы распределения корреляции признаков [8; 9]. Соответственно, состав и структура данных изменяются, и требуется обработка следующим алгоритмом. После данных преобразований необходимо уменьшение размерности, но из-за представления данных в низкоразмерное пространство требуется дополнительное исследование.

Методология

Использование методов и алгоритмов машинного обучения для исследования баз знаний позволяет оптимизировать результат для информационных систем предприятий и внедрить разработки на платформы внутренних структур, например, применение метода самоорганизующихся карт Кохонена в виде кластеризации данных. Нейросеть осуществляет бинарную классификацию, следовательно, определяет, является ли набор сетевых данных стандартным или угрозой для корпоративной сети [10; 11]. Есть множество алгоритмов, которые в связи друг с другом дают высокую вероятность идентификации скрытых атак, например:

- Decision Tree – алгоритм решающих деревьев;
- Random Forest – алгоритм случайного леса;
- алгоритмы экспоненциального смешивания;
- алгоритм обучения Розенблатта;
- другие.

Такие алгоритмы совершенствуют признаки и совместимости значений объекта исследования, что положительно влияет на процесс интеллектуальной обработки данных. В процессе получения новых функций и стратегии поиска уязвимостей решается главный вопрос – составление полных данных для алгоритмов. Чтобы понять, как тот или иной алгоритм ведет себя по отношению к результату, выделяется функция потерь.

Результаты исследования

На данном этапе для продолжения разработки прогнозной модели составлены главные компоненты базы знаний исторических данных [12; 13]. Определенные параметры дают полное образное описание характеристик и присутствие их во внутренней среде предприятий. Таблица ниже показывает наличие или отсутствие событий, совершенных во время трех этапов: во время осуществления скрытых атак, до и после идентификации последствий. Степень проявления характеристик прописана в таблице, то есть если нейросеть показывает высокий процент присутствия угрозы, следовательно, данная характеристика имеет высокую плотность пребывания в модулях информационных систем, и в таблице, соответственно, все плюсы.

Таблица

Параметры исторических данных*

Наименование характеристик	Есть	Перед модификацией	Во время модификации	После модификации
Частая загрузка и выгрузка файлов	+	–	–	+
Внедрение инновационных решений	+	+	+	–
Закрытие отделов	+	–	–	–
Нарушение прав доступа	-	+	+	–
Уровень защищенности	+	+	–	+
n	*n*	*n*	*n*	*n*

**Составлено авторами.*

Такие параметры задают полноценную описательную характеристику происходящих на предприятии событий. Увеличение времени изменений компонентов не должно учитываться в дальнейшем, так как это принесет нежелательный эффект. Использование большого количества признаков сделает нейросеть переобученной, интеллектуальный анализ выдаст много ошибочных заключений [14].

Возникают задачи прикладного характера, связанные с необходимостью усовершенствования анализа внутренних и внешних воздействий на объект исследования с целью обнаружения скрытых угроз:

- анализ факторов и связей с уязвимостями в системах;
- анализ распространения и увеличения рисков на предприятиях;
- сбор, обработка и анализ данных;
- подготовка и нормализация признаков, сокращение объемов неструктурированных данных.

Сама система идентификации признаков построена на бинарных ответах, что не умножает варианты, а объединяет их и выдает результат в краткой форме. Утвердительная или отрицательная форма значений при определении статуса влияния совершаемых действий измеряет в интервале времени уровень воздействия. Каждая структура предприятия имеет последствия в таких областях, как информация, комплексы и сети.

Обработка и анализ данных по перечисленным признакам осуществляются на предприятии с помощью интеллектуальных инструментов исследования критериев. Чтобы создать качественный датасет, потребуется сосредоточиться на характере уязвимостей. Внедрение нейросетей как интеллектуально-прогностического метода позволит с высокой вероятностью обнаружить последствия человеческого фактора на предприятии и об-

наружить цифровой след злоумышленника. Чтобы прийти к данному результату и определению новых характеристик, разрабатывается экспертная оценка узкопрофильным специалистом или обращение к данной области литературы [15; 16].

Применение данных характеристик в последующих исследованиях направит алгоритм поиска в сторону анализа и определения зависимостей между последствиями угроз и скрытыми уязвимостями. Найденные критерии анализа (см. Таблицу) направлены на раскрытие потенциала применяемых алгоритмов машинного обучения. Результаты алгоритма напрямую зависят от используемых данных: если материал позволяет выполнять задачи регрессии, классификации и др., то применение на практике позволит выявить скрытые угрозы, основываясь на новых характеристиках из таблицы.

Выводы и дискуссия

Не все предприятия имеют свою историю благоприятных или неблагоприятных событий, поэтому поиск скрытых атак иногда идет с существенными затруднениями. Во избежание этого и для усовершенствования алгоритма машинного обучения были применены обработка и интеллектуальный анализ исторических данных [17]. На сегодняшний день системы управления событиями безопасности направлены на общую ИТ-инфраструктуру предприятия. Процесс обнаружения строится на сравнении предыдущих инцидентов [18]. Если двигаться по данному направлению, то исследования в области признакового пространства в настоящее время являются актуальным вопросом. Благодаря исследованиям методов интеллектуального анализа и применению алгоритмов классификации и регрессии созданная таблица исторических данных поможет повысить результат прогнозной модели. Чтобы удерживать высокий уровень безопасности данных, необходимо также модернизировать методы идентификации и анализа. Развитие в данном направлении предусматривает рассмотрение всех способов и применимых технологий обнаружения скрытых атак на предприятии.

Существующие решения обнаружения атак основываются на внедрении программно-технических средств и на мерах общего характера защиты. Для определения одиночной скрытой атаки применяемые методы, возможно, будут эффективны, но в условиях длительного действия скрытых угроз нужна оценка обстановки на разных уровнях, то есть анализ признаков всех этапов состояния уязвимости, а также использование прогностической модели. Недостаточно задействовать разрозненные средства защиты в виде программного обеспечения, антивирусов и др. Составление признакового пространства на основе исторических данных предприятия, как показано в таблице, определяет дальнейший путь обнаружения при восстановлении цифрового следа угроз в информационных системах.

Практическая значимость разработки заключается в том, чтобы на основе исследований, разработанных методов и алгоритмов создать систему для предприятия, обеспечивающую высокую надежность и производительность в условиях уязвимости, преднамеренных и неумышленных угроз как с технической, так и с информационной стороны.

Литература

1. *Albanese M., Cam H., Jajodia S.* Automated Cyber Situation Awareness Tools and Models for Improving Analyst Performance // Pino R., Kott A., Shevenell M. (Eds). Cybersecurity Systems for Human Cognition Augmentation. Series: Advances in Information Security. 2014. Vol. 61. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-10374-7_3

2. *Bacciotti A.* Stability and Control of Linear Systems. Series: Studies in Systems, Decision and Control. Springer Cham, 2019. 189 p. DOI: https://doi.org/10.1007/978-3-030-02405-5
3. *Бринк Х. Ричардс Дж. Феверолф М.* Машинное обучение в реальном мире. СПб. : Питер, 2017. 336 с. ISBN: 978-5-496-02989-6.
4. *Burnashev R.A., Gabdrahmanov R.G., Amer I.F. et al.* Research on the Development of Expert Systems Using Artificial Intelligence // Advances in Intelligent Systems and Computing. 2020. Vol. 1051. P. 233–242. DOI: 10.1007/978-3-030-30604-5_21
5. *Бурков А.* Машинное обучение без лишних слов. СПб. : Питер, 2020. 192 с. (Серия «Библиотека программиста»). ISBN: 978-5-4461-1560-0.
6. *Witten I., Eibe F.* Data Mining. Practical Machine Learning Tools and Techniques. 2nd edition. Morgan Kaufmann Publishers, 2005. 560 p. ISBN: 0-12-088407-0.
7. *Dey R., Ray G., Balas V.E.* Stability and Stabilization of Linear and Fuzzy Time-Delay Systems. A Linear Matrix Inequality Approach. Series: Intelligent Systems Reference Library. Vol. 141. Springer Cham, 2017. 267 p. DOI: https://doi.org/10.1007/978-3-319-70149-3
8. *Hastie T., Friedman J., Tibshirani R.* The Elements of Statistical Learning. Data Mining, Inference, and Prediction. Series: Springer Series in Statistics. New York : Springer, 2001. 536 p. DOI: https://doi.org/10.1007/978-0-387-21606-5
9. *Хасти Т., Тибширани Р., Фридман Дж.* Основы статистического обучения: интеллектуальный анализ данных, логический вывод и прогнозирование. 2-е изд. М. : Диалектика-Вильямс, 2020. 770 с. ISBN 978-5-907144-42-2
10. *Зыков С.В.* Основы проектирования корпоративных систем. М. : Изд. дом Высшей школы экономики, 2012. 431 с. ISBN 978-5-7598-0862-6.
11. *Зыков С.В.* Технология интеграции гетерогенного контента в корпоративных информационных системах // Вопросы кибербезопасности. 2015. Т. 4. С. 48–52. EDN UIYNNV.
12. *Luisi J.* Pragmatic Enterprise Architecture. Strategies to Transform Information Systems in the Era of Big Data. 1st edition. Morgan Kaufmann, 2014. 372 p. ISBN 9780128005026.
13. *Xinming Ou, Anoop Singhal.* Quantitative Security Risk Assessment of Enterprise Networks. Series: Springer Briefs in Computer Science. New York : Springer, 2011. 28 p. DOI: 10.1007/978-1-4614-1860-3DOI: 10.1007/978-1-4614-1860-3
14. *Xu Z., Vial R., Kersting K.* Graph Enhanced Memory Networks for Sentiment Analysis // Ceci M., Hollmén J., Todorovski L., Vens C., Džeroski S. (Eds) Machine Learning and Knowledge Discovery in Databases. ECML PKDD 2017. Lecture Notes in Computer Science. Vol. 10534. Cham : Springer, 2017. DOI: https://doi.org/10.1007/978-3-319-71249-9_23
15. *Jones A., Ashenden D.* Risk Management for Computer Security. Protecting Your Network and Information. 1st edition. Butterworth-Heinemann, 2005. 296 p.
16. *Hinkel G.* (2018). NMF: A Multi-platform Modeling Framework // Rensink A., Sánchez Cuadrado J. (Eds) Theory and Practice of Model Transformation. ICMT 2018. Series: Lecture Notes in Computer Science. Vol. 10888. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-93317-7_10
17. *Шелухин О.И.* Сетевые аномалии. Обнаружение, локализация, прогнозирование. М. : Горячая линия-Телеком, 2019. 448 с. ISBN 978-5-9912-0756-0.
18. *Шолле Ф.* Глубокое обучения на Python. СПб. : Питер, 2018. 400 с. ISBN 978-5-4461-0770-4.

References

1. Albanese M., Cam H., Jajodia S. (2014). Automated Cyber Situation Awareness Tools and Models for Improving Analyst Performance. In: Pino R., Kott A., Shevenell M. (Eds) *Cybersecurity Systems for Human Cognition Augmentation*. Series: Advances in Information Security. Vol. 61. Springer, Cham. DOI: 10.1007/978-3-319-10374-7_3
2. Bacciotti A. (2019). *Stability and Control of Linear Systems*. Series: Studies in Systems, Decision and Control. Springer Cham, 189 p. DOI: https://doi.org/10.1007/978-3-030-02405-5
3. Brink H., Richards J., Fetherolf M. (2017) *Real-World Machine Learning*. Shelter Island, NY : Manning Publications Co. (Russian edition: St. Petersburg : Piter Publishing. 336 p. ISBN 978-5-496-02989-6).
4. Burnashev R.A., Gabdrahmanov R.G., Amer I.F. et al. (2020). Research on the Development of Expert Systems Using Artificial Intelligence. *Advances in Intelligent Systems and Computing*. Vol. 1051. P. 233–242. DOI: 10.1007/978-3-030-30604-5_21
5. Burkov A. (2020) *Mashinnoe obuchenie bez lishnikh slov* [Machine learning without unnecessary words]. St. Petersburg : Piter Publishing, 192 p. ISBN 978-5-4461-1560-0 (In Russian).
6. Witten I., Eibe F. (2005). *Data Mining. Practical Machine Learning Tools and Techniques*. 2nd edition. Morgan Kaufmann Publishers, 560 p. ISBN: 0-12-088407-0.
7. Dey R., Ray G., Balas V.E. (2017) *Stability and Stabilization of Linear and Fuzzy Time-Delay Systems. A Linear Matrix Inequality Approach*. Series: Intelligent Systems Reference Library. Vol. 141. Springer Cham. 267 p. DOI: https://doi.org/10.1007/978-3-319-70149-3
8. Hastie T., Friedman J., Tibshirani R. (2001) *The Elements of Statistical Learning. Data Mining, Inference, and Prediction.* Series: Springer Series in Statistics. New York : Springer. 536 p. DOI: https://doi.org/10.1007/978-0-387-21606-5
9. Hastie T. Tibshirani R., Friedman J. (2001). (2020) *Fundamentals of statistical training: Data mining, logical inference and prediction.* New York : Springer, 770 p. DOI: https://doi.org/10.1007/978-0-387-21606-5 (Russian edition: Moscow : Dialektika-Williams, 2020. 770 p. ISBN 978-5-907144-42-2).
10. Zykov S.V. (2012) *Osnovy proektirovaniya korporativnykh sistem* [Fundamentals of corporate systems design]. Moscow : HSE Publishing. 431 p. ISBN 978-5-7598-0862-6 (In Russian).
11. Zykov S.V. (2015) Tekhnologiya integratsii geterogennogo kontenta v korporativnykh informatsionnykh sistemakh [Heterogeneous content integration technology in corporate information systems]. *Voprosy kiberbezopasnosti*. Vol. 4. Pp. 48–52. (In Russian).
12. Luisi J. (2014) *Pragmatic Enterprise Architecture. Strategies to Transform Information Systems in the Era of Big Data*. 1st edition. Morgan Kaufmann. 372 p. ISBN 9780128005026.
13. Xinming Ou, Anoop Singhal (2011). *Quantitative Security Risk Assessment of Enterprise Networks.* Series: Springer Briefs in Computer Science. New York : Springer. 28 p. DOI: 10.1007/978-1-4614-1860-3
14. Xu Z., Vial R., Kersting K. (2017). Graph Enhanced Memory Networks for Sentiment Analysis. In: Ceci M., Hollmén J., Todorovski L., Vens C., Džeroski S. (Eds) *Machine Learning and Knowledge Discovery in Databases. ECML PKDD 2017*. Series: Lecture Notes in Computer Science. Vol. 10534. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-71249-9_23
15. Jones A., Ashenden D. (2005) *Risk Management for Computer Security. Protecting Your Network and Information*. 1st edition. Butterworth-Heinemann. 296 p.
16. Hinkel G. (2018). NMF: A Multi-platform Modeling Framework. In: Rensink A., Sánchez Cuadrado J. (Eds) *Theory and Practice of Model Transformation. ICMT 2018*. Series: Lecture Notes in Computer Science. Vol. 10888. Springer, Cham. DOI: https://doi.org/10.1007/978-3-319-93317-7_10

17. Shelukhin O.I. (2019) *Setevye anomalii. Obnaruzhenie, lokalizatsiya, prognozirovanie* [Network anomalies. Detection, localization, forecasting]. Moscow : Goryachaya liniya-Telekom. 448 p. ISBN 978-5-9912-0756-0. (In Russian).
18. Chollet F. (2018) *Deep Learning with Python*. Shelter Island : Manning Publications. (Russian edition: St. Petersburg: Piter Publishing, 400 p. ISBN 978-5-4461-0770-4).