Scientific journal
PHYSICAL AND MATHEMATICAL EDUCATION
Has been issued since 2013.

Науковий журнал
ФІЗИКО-МАТЕМАТИЧНА ОСВІТА
Видається з 2013.

ISSN 2413-158X (online)
ISSN 2413-1571 (print)

http://fmo-journal.fizmatsspu.sumy.ua/

Рихтер Т.В., Абрамова И.В. Разработка модели информационной безопасности баз знаний. Фізико-математична освіта. 2020. Випуск 1(23). С. 106-110.

Richter T., Abramova I. Development of the model of information security of knowledge. Physical and Mathematical Education. 2020. Issue 1(23). P. 106-110.

DOI 10.31110/2413-1571-2020-023-1-017
УДК 004.65

Т.В. Рихтер
Пермский государственный национальный исследовательский университет, Россия
tatyanarikhter@mail.ru
ORCID: 0000-0002-3698-3147
И.В. Абрамова
Пермский государственный национальный исследовательский университет, Россия
irina-and-denis@yandex.ru
ORCID: 0000-0001-6570-4007

РАЗРАБОТКА МОДЕЛИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАЗ ЗНАНИЙ

АННОТАЦИЯ

Формулировка проблемы. *Любая информация, в том числе и данные баз знаний, обладают такими свойствами, как конфиденциальность, целостность и доступность, что указывает на большую значимость задач по ее защите. Современная практика показывает, что в настоящее время все чаще возникают проблемы необходимости создания комплекса дополнительных аппаратных и программных средств защиты баз знаний от несанкционированного доступа или подключения.*

Материалы и методы: *теоретический анализ и обобщение научно-исследовательских работ, значимость которых признана научным сообществом в сфере системы обеспечения информационной безопасности в базах знаний.*

Результаты. *Разработана модель информационной безопасности баз знаний, включающая следующие составляющие: цель (обеспечение информационной безопасности баз знаний); задачи (обеспечение целостности данных в базах знаний, конфиденциальности информации, ее доступности для авторизованных пользователей); функции защиты информации в базах знаний; программные решения (обнаружение и оценка; управление правами доступа в рамках мандатной и дискреционной защиты; мониторинг и блокирование; аудит; защита данных; безопасность нетехнического характера); методы защиты баз знаний (использование актуальных версий информационных потоковых программ; применение последних версий браузеров; наличие дополнительного программного обеспечения, проверяющее поле загрузки и запросы); технико-экономические показатели методов защиты информации в базах знаний (вероятность «взлома» защиты злоумышленниками; безопасное время; стоимость разработки и внедрения системы защиты, эксплуатационные затраты; минимальное количество несанкционированных обращений пользователей к различным защищенным ресурсам баз знаний).*

Выводы. *Выбранные в модели методы защиты обеспечивают экстремальные значения показателей эффективности функционирования проектируемой системы защиты базы знаний. Анализ их эффективности является сложным и трудоемким процессом.*

КЛЮЧЕВЫЕ СЛОВА: *информационная безопасность, базы данных, базы знаний, методы защиты информации, модель информационной безопасности баз знаний.*

ВВЕДЕНИЕ

Постановка проблемы. Базы знаний являются основным ядром интеллектуальных информационных систем. Любая информация, в том числе и данные баз знаний, обладают такими свойствами, как конфиденциальность, целостность и доступность, что указывает на большую значимость задач по ее защите. Основные требования, которые предъявляются в процессе защиты баз знаний, во многом совпадают с требованиями, предъявляемыми к безопасности информации в базах данных. Современная практика показывает, что в настоящее время все чаще возникают проблемы необходимости создания комплекса дополнительных аппаратных и программных средств защиты баз знаний от несанкционированного доступа или подключения.

Актуальность исследования. В соответствии с программой «Цифровая экономика Российской Федерации» информационная безопасность относится к одному из пяти базовых направлений развития цифровой экономики. Любая информация имеет три главных свойства, к которым можно отнести конфиденциальность, целостность и доступность, что

указывает на большую значимость задачи по защите информации, являющейся одной из первостепенных в современном обществе. Проблема защиты баз знаний является актуальной в связи с широким внедрением к ним многопользовательского сетевого доступа.

Цель статьи. Цель исследования заключается в разработке модели информационной безопасности баз знаний.

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ

Анализ актуальных исследований. Различные аспекты обеспечения информационной безопасности баз знаний и баз данных рассмотрены в исследованиях таких авторов, как А. Арджомандифард, А.Н. Аюпова, В.В. Баранов, М.А. Бирюков, Е.В. Данилин, И.В. Заводцев, Р.И. Захарченко, С.В. Казмирчук, А.Г. Корченко, Е.А. Костина, С.А. Кравченко, А.С. Максимов, Т.В. Панивко, И.Б. Саенко, С.Н. Федирко, И.Е. Филиппов,П.Ю. Филяк, С.В. Ченушкина, и др.

П.Ю. Филяк, С.Н. Федирко, Е.А. Костина рассматривают подходы к обеспечению информационной безопасности с использованием графовых баз данных и графовых систем представления и управления знаниями, реализованные посредством инструментальных средств на примере решения задачи построения правового поля информационной безопасности организации (Филяк & Федирко & Костина, 2017).

В.В. Кульба и Н.П. Курочка в своей работе выделяют следующие группы методов защиты баз данных (Кульба & Курочка, 2015):

– организационные (ограничение лиц, получающих доступ в вычислительные центры);

– процедурные (наличие доступа к данным и передачи информации лицам, имеющим соответствующее разрешение);

– структурные (структуризация данных с повышенным уровнем защищенности хранимой информации на этапе проектирования структуры базы данных);

– аппаратные (комплекс электронных устройств, встраиваемых в технические средства вычислительных систем или сопрягаемых с ними через стандартный интерфейс);

– программные (комплекс специальных программ, используемых для обеспечения безопасности данных).

В.В. Кульба и Н.П. Курочка рассматривают следующие технико-экономические показатели методов защиты информации в базах данных (Кульба & Курочка, 2015):

– система затрат, необходимых для разработки методов защиты информации в базах данных и при их эксплуатации;

– безопасное время (математическое ожидание времени «взлома» метода защиты через опробование всевозможных вариантов проникновения).

С.В. Ченушкина, И.Е. Филиппов, А.Н. Аюпова с целью обеспечения безопасности баз данных выделяют шесть основных категорий программных решений:

– средства обнаружения и оценки;

– средства для управления правами доступа в рамках мандатной и дискреционной защиты;

– средства мониторинга и блокирования;

– средства аудита;

– средства защиты данных;

– меры безопасности нетехнического характера (Ченушкина & Филиппов & Аюпова, 2017).

Опарина Т.М. предлагает в модели защиты информации в базах данных использовать две основные сущности (Опарина, 2004):

– субъекты (пользователи или группы пользователей);

– объекты (базы данных, имеющие поля и записи).

Каждый пользователь или группа пользователей имеет уровень благонадежности доступа, а каждый объект обладает соответствующей меткой секретности, имеющей следующие составляющие:

– уровень (компонент, принимающий значение конфиденциальности);

– категория (определение принадлежности данных к определенным проектам или отделам);

– группа (задание подмножества лиц, которые имеют доступ к данным).

А.В. Роднин и В.Ю. Турчик выявляют комплекс следующих требований к средствам защиты информации, которые основаны на интеллектуальном анализе действий пользователей в базах данных, учитывая эволюционные характеристики угроз информационной безопасности (Роднин & Турчик, 2015):

– высокий уровень интеграции с бизнес-системами заказчиков;

– память и возможность прогнозирования возникновений угроз;

– адаптивность по отношению к внешней среде;

– управление событиями безопасности и формирование реакции;

– расширенный мониторинг событий безопасности и их протоколирование.

Авторами предложена структурная модель решения обозначенной проблемы, включающая следующие подсистемы: аутентификации, хранения данных, мониторинга и журналирования, аналитики, формирования реакции.

МЕТОДЫ ИССЛЕДОВАНИЯ: теоретический анализ и обобщение научно-исследовательских работ, значимость которых признана научным сообществом в сфере системы обеспечения информационной безопасности в базах знаний.

РЕЗУЛЬТАТЫ ИССЛЕДОВАНИЯ

Базы знаний являются важнейшими интеллектуальными ресурсами, которые должны быть соответствующим образом защищены посредством комплекса определенных средств контроля. Выделены следующие угрозы: похищение

и фальсификация данных в базах знаний; утрата конфиденциальности (нарушение тайны); нарушение неприкосновенности личных данных; утрата целостности; потеря доступности.

Под безопасностью баз знаний будем понимать защиту данных от случайного или преднамеренного разрушения или модификации информации.

Опираясь на исследования российских и зарубежных исследований в области информационной безопасности, разработана модель информационной безопасности баз знаний, включающая цель, задачи, функции защиты информации в базах знаний, принципы обеспечения информационной безопасности баз знаний, программные решения, методы защиты баз знаний, технико-экономические показатели методов защиты информации в базах знаний (рис. 1).

Модель поддерживает избирательный подход к вопросу обеспечения безопасности данных в базе знаний. Пользователи обладают различными правами (привилегиями или полномочиями) при работе с данными объектами. Избирательные права характеризуются значительной гибкостью.

С целью реализации в модели избирательного принципа предусмотрен следующий метод: база знаний постоянно пополняется новыми типами объектов (пользователями), каждый из которых обладает уникальными идентификаторами. При дополнительной защите все пользователи кроме уникального идентификатора получают уникальные пароли.

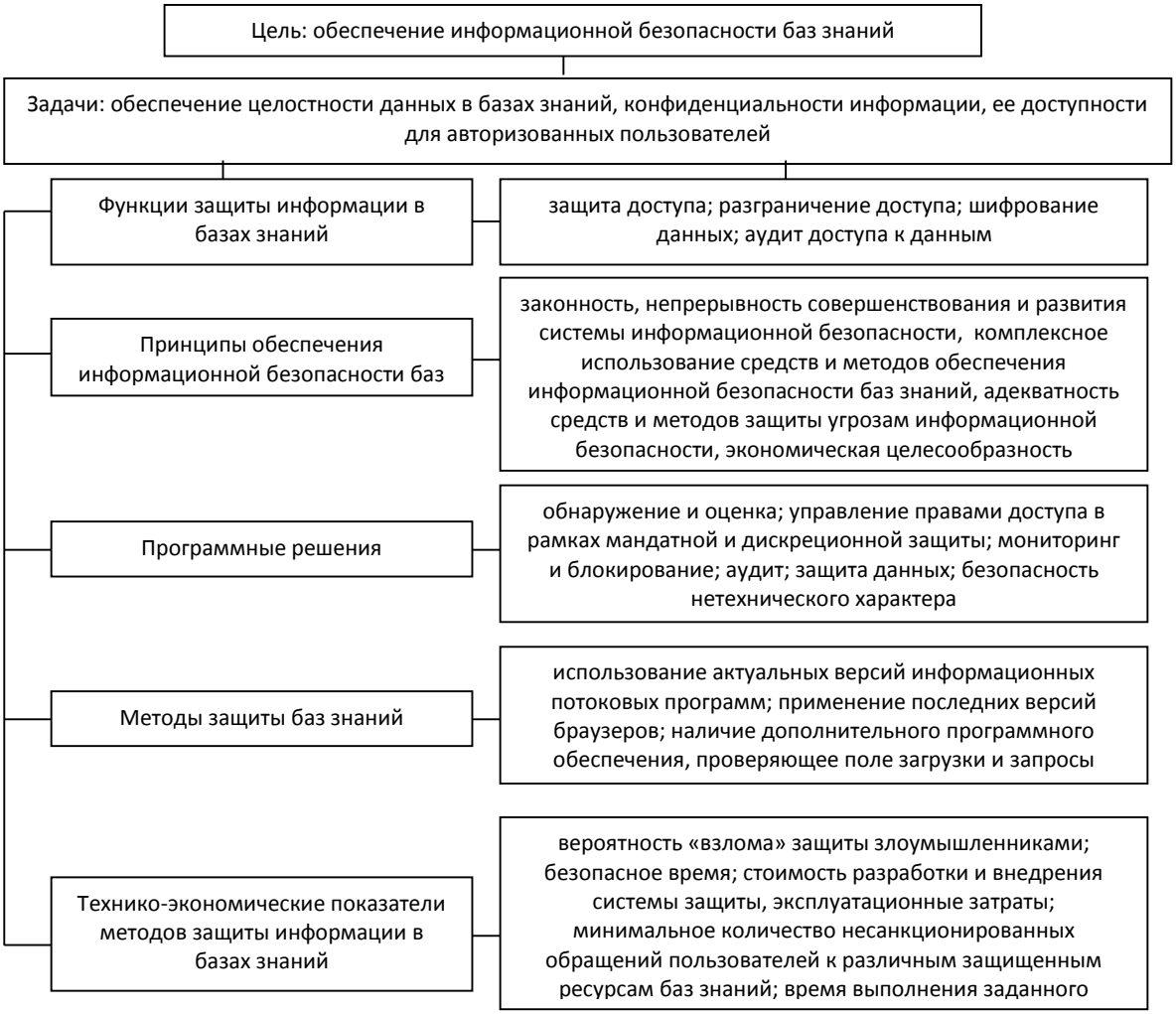

Рис. 1. Модель информационной безопасности баз знаний

Цель модели: обеспечение информационной безопасности баз знаний.

Задачи модели: обеспечение целостности данных в базах знаний, конфиденциальности информации, ее доступности для авторизованных пользователей.

Функции защиты информации в базах знаний:

– защита доступа;

– разграничение доступа;

– шифрование данных;

– аудит доступа к данным.

Принципы обеспечения информационной безопасности баз знаний: законность, непрерывность совершенствования и развития системы информационной безопасности, комплексное использование средств и методов обеспечения информационной безопасности баз знаний, адекватность средств и методов защиты угрозам информационной безопасности, экономическая целесообразность.

С целью обеспечения безопасности баз знаний выделены следующие программные решения:

– обнаружение и оценка (выявление уязвимостей баз знаний, местонахождение критически важных данных);

– управление правами доступа в рамках мандатной и дискреционной защиты;

– мониторинг и блокирование (защита баз знаний от взлома, неавторизированного доступа и похищения информации);

– аудит (подтверждение соответствия информационной системы отраслевым стандартам безопасности);

– защита данных (целостность и конфиденциальность данных в базах знаний);

– безопасность нетехнического характера (повышение культуры обращения с конфиденциальными данными и степень готовности к угрозам).

Методы защиты баз знаний:

– использование актуальных версий информационных потоковых программ;

– применение последних версий браузеров;

– наличие дополнительного программного обеспечения, проверяющее поле загрузки и запросы.

Механизм защиты базы знаний – обеспечение доступа и допуска к информации лиц, обладающих соответствующими полномочиями.

Технико-экономические показатели методов защиты информации в базах знаний:

– вероятность «взлома» защиты злоумышленниками;

– безопасное время;

– стоимость разработки и внедрения системы защиты, эксплуатационные затраты;

– минимальное количество несанкционированных обращений пользователей к различным защищенным ресурсам баз знаний;

– время выполнения заданного множества запросов пользователей.

Основной результат внедрения разработанной модели информационной безопасности баз знаний предполагает значительное снижение рисков утечки конфиденциальной информации как от внешний нарушителей, так и от легальных пользователей.

ОБСУЖДЕНИЕ

В статье рассматриваются некоторые аспекты актуальной в настоящее время проблемы разработки модели информационной безопасности баз знаний с целью снижения вероятности получения несанкционированного доступа к имеющимся в них данных. К основным угрозам информационной безопасности в базах знаний относят разграничение прав доступа, передачу информации по каналам связи и работу в сети Интернет, злонамеренную модификацию параметров функционирования базы знаний внутренним нарушителем, несанкционированный доступ к конфиденциальной информации.

Можно выделить следующие основные средства защиты данных в базах знаний: вхождение по паролю (введение определенной комбинации символов); разграничение прав доступа к объектам базы знаний; шифрование данных в базах знаний.

Анализ литературы по проблеме выявления средств и способов защиты информации в базах знаний позволил систематизировать их в следующие группы:

1. Средства защиты: технические: физические и аппаратные (брандмауэры, фильтры, сетевые экраны, устройства шифрования протокола и др.); программные (антивирусные программы, средства идентификации и аутентификации пользователей, протоколирование и аудит, мониторинг баз знаний, средства архивации данных, криптографические средства, средства управления доступом и др.); социально-правовые (организационные, законодательные, морально-этические).

2. Способы защиты: регламентация, побуждение, принуждение, управление доступом, препятствие, маскировка информации, противодействие вирусам и др.

Выделены основные виды угроз для баз знаний:

– осуществление неумышленных или некомпетентных действий;

– несанкционированный обмен информацией между пользователями;

– несанкционированный межсетевой доступ к информационным и техническим ресурсам баз знаний;

– разглашение, передача, утрата ключей, паролей, программ;

– внесение изменений в имеющуюся архитектуру баз знаний;

– отключение, расшифровка средств и методов защиты;

– использование некорректных данных, режимов работы, адресов и т.д.;

– распространение сетевых вирусов.

ВЫВОДЫ И ПЕРСПЕКТИВЫ ДАЛЬНЕЙШЕГО ИССЛЕДОВАНИЯ

В результате выполненного исследования разработана модель информационной безопасности баз знаний, поскольку своевременная информационная безопасность является важнейшим условием защиты информации любой интеллектуальной системы. Выбранные в модели методы защиты обеспечивают экстремальные значения показателей эффективности функционирования проектируемой системы защиты базы знаний. Анализ их эффективности является сложным и трудоемким процессом. Полученные результаты целесообразно применять при разработке политики безопасности учреждения в условиях информационной борьбы. К перспективам дальнейшего исследования можно отнести разработку модели информационной безопасности в компьютерных сетях.

Список использованных источников

1. Кульба В.В., Курочка Н.П. Математическая модель обеспечения безопасности информации в базах даных. *Интернет-журнал Науковедение*, 2015. Т. 5. № 3(28). С. 108. URL: https://elibrary.ru/item.asp?id=24321509 (Дата обращения 14.02.2020).

2. Опарина Т.М. Модель автоматической защиты информации в базе данных от получения данных с помощью логических выводов. *Математические структуры и моделирование*, 2004. № 14. С. 123-127. URL: https://elibrary.ru/item.asp?id=21994769 (Дата обращения 17.02.2020).
3. Роднин А.В., Турчик В.Ю. Концепция применения интеллектуального анализа данных в средствах защиты информации баз данных. Физика. Технологии. Инновации: сборник научных трудов. Министерство образования и науки Российской Федерации, Уральский федеральный университет. 2015. С. 263-269. URL: https://elibrary.ru/item.asp?id=25153166 (Дата обращения 12.02.2020).
4. Филяк П.Ю., Федирко С.Н., Костина Е.А. Обеспечение информационной безопасности с помощью графовых баз данных и графовых систем представления и управления знаниями. *Информация и безопасность*, 2017. Т. 20. № 2. С. 285-288. URL: https https://elibrary.ru/item.asp?id=29315871 (Дата обращения 19.02.2020).
5. Ченушкина С.В., Филиппов И.Е., Аюпова А.Н. Защита баз данных, как актуальное направление в структуре информационной безопасности. European research: сборник статей победителей X Международной научно-практической конференции. 2017. С. 169-172. URL: https://elibrary.ru/item.asp?id=29224861 (Дата обращения 22.02.2020).

References

1. Kul'ba, V.V., Kurochka, N.P. (2015). Matematicheskaja model' obespechenija bezopasnosti informacii v bazah dannyh [A mathematical model for ensuring the security of information in databases]. *Internet-zhurnal Naukovedenie - Internet Journal of Science*, T. 5, 3(28), 108. Retrieved from https://elibrary.ru/item.asp?id=24321509 [in Russian].
2. Oparina, T.M. (2004). Model' avtomaticheskoj zashhity informacii v baze dannyh ot poluchenija dannyh s pomo-shh'ju logicheskih vyvodov [A model of automatic protection of information in a database from receiving data using logical inferences]. *Matematicheskie struktury i modelirovanie - Mathematical Structures and Modeling*, 14, 123-127. Retrieved from https://elibrary.ru/item.asp?id=21994769 [in Russian].
3. Rodnin, A.V., Turchik, V.Ju. (2015). Koncepcija primenenija intellektual'nogo analiza dannyh v sredstvah zashhity informacii baz dannyh [The concept of the use of data mining in the means of protecting database information]. *Fizika. Tehnologii. Innovacii - Physics. Technology*. *Innovation*: sbornik nauchnyh trudov. Ministerstvo obrazovanija i nauki Rossijskoj Federacii, Ural'skij federal'nyj universitet, 263-269. Retrieved from https://elibrary.ru/item.asp?id=25153166 [in Russian].
4. Filjak, P.Ju., Fedirko, S.N., Kostina, E.A. (2017). Obespechenie informacionnoj bezopasnosti s pomoshh'ju grafovyh baz dannyh i grafovyh sistem predstavlenija i upravlenija znanijami [Ensuring information security using graph databases and graph representation and knowledge management systems]. *Informacija i bezopasnost' - Information and Security*, T. 20, 2, 285-288. Retrieved from https://elibrary.ru/item.asp?id=29315871 [in Russian].
5. Chenushkina, S.V., Filippov, I.E., Ajupova, A.N. (2017). Zashhita baz dannyh, kak aktual'noe napravlenie v strukture informacionnoj bezopasnosti [Database protection as an actual direction in the structure of information security]. *European research- European research*: sbornik statej pobeditelej H Mezhdunarodnoj nauchno-prakticheskoj konferencii, 169-172. Retrieved from https://elibrary.ru/item.asp?id=29224861 [in Russian].

DEVELOPMENT OF THE MODEL OF INFORMATION SECURITY OF KNOWLEDGE

Tatiana Richter, Irina Abramova

Perm State National Research University, Russia

Abstract.

Formulation of problem. *Any information, including knowledge base data, has such properties as confidentiality, integrity, and accessibility, which indicates the great importance of the tasks for its protection. Modern practice shows that nowadays more and more problems arise with the need to create a set of additional hardware and software tools for protecting knowledge bases from unauthorized access or connection.*

Materials and methods*: theoretical analysis and generalization of research projects, the importance of which is recognized by the scientific community in the field of information security in the knowledge base.*

Results. *A model of information security of knowledge bases have been developed, including the following components: goal (ensuring information security of knowledge bases); tasks (ensuring data integrity in knowledge bases, the confidentiality of information, its availability for authorized users); information protection functions in knowledge bases; software solutions (detection and evaluation; management of access rights within the framework of mandatory and discretionary protection; monitoring and blocking; audit; data protection; non-technical security); methods for protecting knowledge bases (using up-to-date versions of informational streaming programs; using the latest browser versions; the presence of additional software that checks the download field and queries) technical and economic indicators of information protection methods in knowledge bases (the probability of "hacking" of protection by cybercriminals; safe time; the cost of developing and implementing a protection system, operating costs; the minimum number of unauthorized users accessing various protected knowledge base resources).*

Conclusions. *The protection methods selected in the model provide extreme values of the performance indicators of the designed knowledge base protection system. Analysis of their effectiveness is a complex and time-consuming process.*

Keywords: *information security, databases, knowledge bases, information protection methods, the information security model of knowledge bases.*