 DOI 10.25699/SSSB.2019.2(26).32514

05.13.18

РАЗРАБОТКА ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ РЕАЛИЗАЦИИ ПРОЦЕССА АУДИТА СОСТОЯНИЯ ЗАЩИЩЁННОСТИ ИНФОРМАЦИИ

Е.В. Трапезников

ФГБОУ ВО «Омский государственный технический университет» (ОмГТУ), г. Омск

Развитие технологий обработки и хранения информации влечёт за собой появление новых угроз и уязвимостей. Для предотвращения потери информации развиваются как средства защиты, так и нормативно-правовая база. Используемые средства защиты должны обеспечивать необходимый уровень защиты. Подтвердить данный уровень или оповестить о его недостатках позволяет своевременно проведённый аудит. В статье рассмотрен вопрос разработки программного обеспечения для реализации процесса аудита системы защиты автоматизированных систем. Представлена разработанная модель оценки защищённости информации с использованием интеллектуальных средств. Разработан и реализован алгоритм программного обеспечения для проведения аудита состояния защищённости автоматизированной системы для специалиста по информационной безопасности. Приведены предварительные данные апробации разработанного алгоритма и программного комплекса.

Ключевые слова: аудит, автоматизированная система, свойства информации, менеджмент безопасности, модель информационной безопасности, MVC, ORM.

ВВЕДЕНИЕ

В период активного внедрения и использованию информационных технологий в различных сферах жизнедеятельности человека появляются различные угрозы безопасности и целостности используемых данных.

В период жизненного цикла информации – от получения, до хранения и уничтожения – необходимо проводить аудит качества обеспечения информационной безопасности, для предотвращения потери информации в любой из периодов. Качественно проведённый аудит определяет соответствие нормативно-правовой составляющей и определяет, в какой степени аппаратно-программный комплекс защиты информации организации находится в актуальном состоянии.

Проблемами аудита и обеспечения информационной безопасности в настоящий момент посвящены работы ряда российских учёных таких как: Васильев В.И., Глушенко С.А., Долженко А.И., Салова В.В., А.А. Шелупанов и т.д. Работы рядя зарубежных авторов также посвящены вопросам обеспечения защиты информации и аудита систем защиты.

В настоящий момент информация является одним из основных активов, которые обладает особой ценностью и должен быть надлежащим образом защищён [1]. Вследствии этого возникает проблема появления большего числа угроз и уязвимостей. Любая проблема в системе защите автоматизированной системе привод к нарушению трех основных свойств информации:

1. Конфиденциальность – гарантирует доступ к информации определённому кругу лиц.

2. Целостность – гарантирует, что только определённый круг лиц может изменять информацию

3. Доступность – гарантирует беспрепятственный и постоянный доступ к информации определённому кругу лиц.

При построении систем информационной безопасности важное значение имеют процессы контроля адекватность мер и средств защиты, а также выявление уязвимостей в существующей информационной системе. Аудит информационной безопасности позволяет провести такой контроль и выявить новые уязвимости [2,3,4,5,6,7].

Научная школа профессора А.А. Шелупанова активно занимается вопросами проектирования систем защиты с использованием различных моделей построения защиты информации [8]. Авторы проводят исследования, направленные на реализацию и улучшения различных типов механизмов защиты информации. Авторы рассматривают вопрос оценки защищённости информации, в частности разработана модель документооборота, которая предполагает действия на информацию в абсолютно различных средах [9].

Возросшие экономические потери на фоне слабой системы защиты информации и не своевременно проведённого аудита отражены во многих работах [10, 11, 12]. Авторы [10] приводят рассмотрение вопроса о влиянии взаимосвязи между внутренним аудитом и функциями информационной безопасности. В работе приведена исследовательская модель, отражающая составляющие системы аудита.

В момент проведения аудита авторы [13, 14] предлагают интегрировать в процесс пользователей, для определения конкретных человеческих факторов и возможных рисков. Помимо этого авторы предлагают

повсеместно внедрять систему активного мониторинга. Постоянный мониторинг позволят проводить аудит системы защиты не прекращая работу системы в целом.

В работе [15] авторы разработали модель, включающая множество аспектов обеспечения безопасности, включая атак, обнаружения, восстановления, оценкой рисков и снижения уязвимости. Моделирование системы с использованием разработанной модели позволяет рассматривать динамику системы. Часть исследований направлена на разработку модели оценки необходимости и эффективности проведения аудита информационных систем [16, 17].

ОСНОВНАЯ ЧАСТЬ

В результате анализа исследований предметной области были определены следующие задачи: разработка процесса аудита и модели оценки защищённости информации с элементами интеллектуальных средств, обеспечивающие помощь в принятии решения. Модель является основной для алгоритма и реализации программного обеспечения для специалиста по информационной безопасности, создаваемого в целях анализа и оценки качества защищённости информации в автоматизированной системе. Решаемые задачи обосновываются актуальностью представленной темы в связи развитием технологий и повсеместным внедрением информационных технологий для обработки, хранения и передачи информации.

Задачей разработки модели для проведения аудита состояния защищённости информации ставится получение алгоритма, позволяющего повысить качества и скорость проведения аудита. Помимо этого, алгоритм должен содержать возможность самостоятельного принятия решений в определённых случаях. Для решения поставленной задачи использованы следующие способы и методы: теория алгоритмов, технология баз данных, метод экспертных оценок, теория искусственного интеллекта, методология защиты, объектно-ориентированного программирования. Модель предполагает, что система должна в полной мере удовлетворять требования законодательства в области системы защиты информации. Оценка защищённости формируется с использованием критериев ГОСТ Р ИСО/МЭК 15408 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» [18].

Для разработки модели оценки защищённости информации использована блочная структура построения системы (рис. 1).

Согласно представленной схеме имеются семь основных блоков, которые определённым образом взаимосвязаны между собой, обмениваясь тем самым информацией в процессе жизненного цикла:

- блок «Анализ входных данных»;
- блок «Библиотека»;
- блок «База данных»;
- блок «Оценка защищённости»;
- блок «Формирования перечня угроз»;
- блок «Интеллектуальные средства»;
- блок «Выдача результатов»

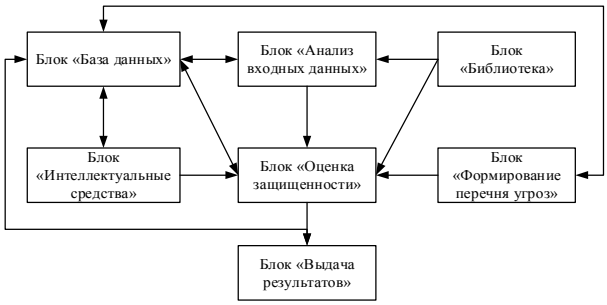

Рис. 1. Схема модели

Первоначально весь сбор информации начинается в блоке «Анализ входных данных» (рис. 2). С помощью данного этапа определяется состав исследуемой системы (программное обеспечение, аппаратное обеспечение, информационные базы, документация, существующее или предполагаемое (или существующее) сетевое взаимодействие). Определение составляющих системы защиты, текущие настройки, уровни доступа и т.д. проводится на основе анкетирования. Для анкетирования формируются перечень опросных листов. Полученные результаты анкетирования формируют часть входных данных для блока «Интеллектуальные средства».

Формирование основных (необходимых) требований для системы защиты информации определяется на основе класса используемой автоматизированной системы, определённый в соответствии с соответствующими документами.

В работе рассматривается и определяется класс автоматизированной системы на основе руководящего документа Федеральной службу по техническому и экспортному контролю «Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации» [19].

Следующие параметры служат для определения класса:

1. Уровень конфиденциальности информации.
2. Уровень доступа к конфиденциальной информации.
3. Режим обработки данных.

Информация, которая формируется для аудита и оценки защищённости заносится, либо выгружается из блока «База данных».

Дополнительными требования к классу автоматизированной системы формируются на основе приказа ФСТЭК России от 11 февраля 2013 г. N 17 и других руководящих документов ФСТЭК [20].

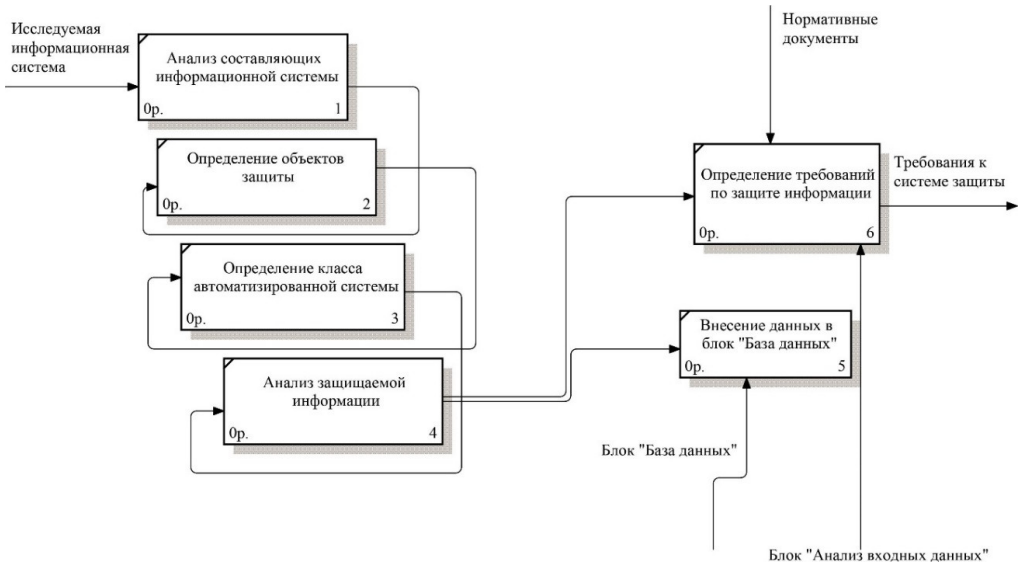

Рис. 2. Диаграмма блока «Анализ входных данных»

Согласно приказу «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» [20]:

Класс защищенности (К) = [уровень значимости информации; масштаб системы]

где

УЗ = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)]

Вся необходимая документация, которая используется на протяжении всей схемы модели, формируется из блока «Библиотека».

Сформированные результаты подготовительного этапа позволяют сформировать перечень дестабилизирующих факторов на основе банка данных ФСТЭК, локальная копия хранится внутри блока «База данных».

$$S = \{s_1, ..., s_N\}$$

где S – множество дестабилизирующих факторов.

Блок «Оценка защищённости» содержит в себе элементы теории искусственных нейронных сетей. Для данного блока формируется входной вектор, который содержит результаты предыдущих этапов и перечень дестабилизирующих факторов. Все сформированные данные помогают интеллектуальной среде выполнить принятие решений.

В данном блоке формируются векторы для входного и выходного слоя нейронной сети. Каждый дестабилизирующий фактор обладает своим весовым коэффициентом, который может меняться в процессе обучения нейронной сети.

Выходной слой нейронной сети содержит результаты принятия решений о возможных угрозах системы.

Обучения происходит по методу «с учителем». Нейронная сеть принимает решение о необходимых мероприятиях, в зависимости от возможных дестабилизирующих факторов.

Результирующим блоком всей модели является блок «Выдача результатов». На данном этапе формируются необходимые документы о недостатках системы и мерах по её устранению. Приводятся ссылки на пункты нормативно-правовой документации, если это необходимо.

ПРОГРАММНАЯ РАЗРАБОТКА

Программная реализация строится на постепенном сборе информации об объекте информатизацией для последующей оценки защищённости (выполнения аудита) и формировании результатов (рис. 3.).

Программная реализация выполнена с использованием языка программирования C# (объектно-ориентированное программирование) и среды разработки Microsoft Visual Studio 2017. Программное обеспечение имеет в своём составе базу данных, как основное хранилище всей информации, циркулирующей внутри разработки. Так как на данный момент предполагается использование локальной базы данных без установки стороннего программного обеспечения, то для реализации выбрана встраиваемая кроссплатформенная база данных SQLite, которая поддерживает достаточной полный набор команд языка SQL.

Взаимодействие с базой данных осуществляется средствами ORM технологии. Данная технология позволяет взаимодействовать с базой данных по принципу ООП. Запросы к базе выполняются через модели по средствам LINQ.

Программное обеспечение строится на основе патерна разработки MVC – model, view, controller. Основная логика разработки и визуальное представле-

ниеразделяются, обеспечивая тем самым масштабируемость разработки и удобства в переносе. Для обеспечения независимости расчётов и получения результатов от различных блоков алгоритма, отдельные процессы выделяются в собственные независимые потоки.

Работа с программным обеспечением строится на использовании возможности разграничения прав доступа. Назначенные права определяются в зависимости от того, какой пользователь авторизовался в системе. После авторизации в системе пользователь может приступить к работе. Пароли пользователей хранятся в базе в зашифрованном виде, обеспечивая тем самым безопасность работы с программным обеспечением.

На первом этапе идёт создание или открытие уже существующего проекта. Проект создаётся под каждую исследуемую систему защиты.

«Проект» является основным понятием в разработанном программном обеспечении. «Проект» содержит информацию о каждой итерации аудита, результаты аудита, результаты запуска интеллектуальных средств и т.д.

При создании «проекта» доступ к нему обеспечивается только администратору системы и пользователю, который его создал. Пользователь в праве предоставить доступ иным лицам к текущему проекту с правами только на чтение.

Первым этапом в работе программного обеспечения является определение класса исследуемой автоматизированной системы. Для определения класса предлагается ответить на ряд вопросов, составленных в соответствии с руководящим документом ФСТЭК. Специалист по информационной безопасности должен правильно оценить класс для того, чтобы должным образов произвести аудит системы защиты и оценку защищённости информации.

На основе подготовительного этапа производится анкетирование и формируются результаты. Полученные результаты являются входными данными для интеллектуального блока.

Отдельным этапом в базу данных программного обеспечения загружается или обновляется перечень актуальных угроз и уязвимостей из Банка данных ФСТЭК. Из данного перечня формируется множество дестабилизирующих факторов.

В результате выполнения всех операций программное обеспечение формирует отчётные документы, в которых отражены все результаты, не соответствия требованиям законодательства и руководящих документов, перечень возможных угроз, которым может быть подвержена автоматизированная система, при текущем состоянии.

Для подтверждения результатов был проведён ряд экспериментов. Объект исследования – система защиты информации организации. Для проведения анализ были использованы данные 20 организаций, в каждой организации были определены различные классы автоматизированных систем.

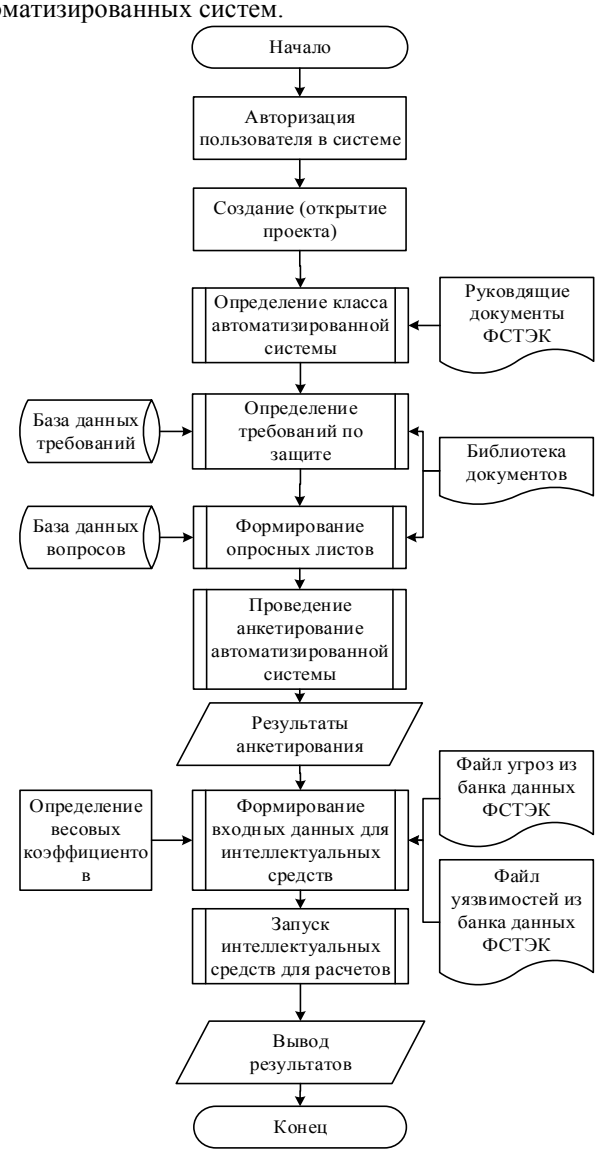

Рис. 3. Блок-схема программного обеспечения

Для каждой организации был проведён полный цикл исследований. В соответствии с которым были получены следующие результаты соответствия систем защиты организаций эталону. Эталонная система – система защиты с полным соответствием требования законодательства (рис. 4).

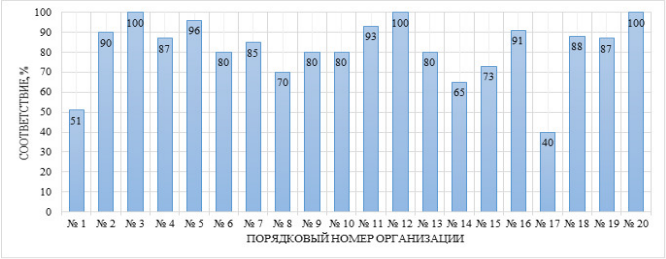

Рис. 4. Результаты исследований

В исследовании видно, что почти все организации содержат достаточно качественную систему защиты, за исключением отдельных. Процент соответствия определяет способность системы защиты отражать возможные атаки с определённой долей вероятности. На основе полученных результатов определялся перечень угроз и уязвимостей, возможных для каждой из систем. Для повышения точности принятие решения нейронной сетью происходило обучение на основе входного вектора и корректировки весовых коэффициентов.

ЗАКЛЮЧЕНИЕ

Развитие технологий и их повсеместное внедрение требует особое внимание к системам защиты информации. В работе рассмотрена реализация процесса аудита на основе модели, основывающейся на возможности принятия решения с помощью нейронной сети. В ходе исследования решены следующие задачи:

1. Предложена модель оценки защищенности информации в автоматизированной системе на основе нейронной сети.
2. Определён перечень документов, на основе которых происходит определение класса автоматизированной системы.
3. Определены требования по соответствию системы защиты информации автоматизированной системы.
4. Представлены диаграмма процесса аудита защищённости.
5. Представлено разработанное программное обеспечения специалиста информационной безопасности для проведения аудита защищённости автоматизированной системы.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менедж-мента информационной безопасности. М.: Стандартинформ, 2014. 210 с.

2. Салова В.В. Интеллектуальная система поддержки принятия решений по проведению аудита информационных систем персональных данных / В.В. Салова, В.И. Васильев // Вестник УГАТУ. – 2014. Т.18, № 3 (64). С. 261-269

3. Глушенко С.А. Система поддержки принятия решений нечеткого моделирования рисков информационной безопасности организации / С.А. Глушенко, А.И. Долженко // Информационные технологии. – 2015. Т.21, № 1. С. 68-74

4. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий / С.И. Макаренко // Системы управления, связи и безопасности. 2018. № 1. С. 1-29

5. Dor D. A model of the information security investment decision-making process / D. Dor, Y. Elovici // Computers & Security. 2016. Vol. 63. С. 1-13

6. Трапезников Е.В. Анализ решений для оценки защищенности информации в информационных системах / Е.В. Трапезников // Россия молодая: передовые технологии – в промышленность! 2017. № 2. С. 30-34

7. Максименко В.Н. Основные подходы к анализу и оценке рисков информационной безопасности / В.Н. Максименко, Е.В. Ясюк // Экономика и качество систем связи. – 2017. № 2 (4). С. 42-48

8. Актуальные направления развития методов и средств защиты информации / А.А. Шелупанов, О.О. Евсютин, А.А. Конев, Е.Ю. Костюченко, Д.В. Кручинин, Д. С. Никифоров // Доклады Томского государственного университета систем управления и радиоэлектроники. 2017. Т. 20, № 3. С. 11–24

9. Новохрестов А.К. Модель угроз безопасности ин-формации и ее носителей / Новохрестов А.К., Конев А.А., Шелупанов А.А., Егошин Н.С. // Вестник Иркутского государственного технического университета. 2017. Т. 21. № 12 (131). С. 93-104

10. The influence of a good relationship between the inter-nal audit and information security functions on information security outcomes / P.J. Steinbart, R. L. Raschke, G. Gal, W. N. Dilla // Accounting, Organizations and Society. 2018

11. Wei Y.-C. Performance evaluation of the recommendation mechanism of information security risk identification : Ad-vances in Human-like Intelligence towards Next-Generation Web / Y.-C. Wei, W.-C.Wu, Y.-C. Chu // Neurocomputing. 2018. Vol. 279. P. 48-53

12. Piech H. Audit expert system of communication security assessment: Knowledge-Based and Intelligent Information & Engineering Systems: Proceedings of the 21st International Conference, KES-20176-8 September 2017, Marseille, France / H. Piech, G. Grodzki // Procedia Computer Science. 2017. Vol. 112. P. 147-156

13. Ki-Aries D. Persona-centred information security awareness / D. Ki-Aries, S. Faily // Computers & Security. 2017. Vol. 70. P. 663-674

14. Boiko A. System Integration and Security of Information Systems : ICTE 2016, Riga Technical University, Latvia / A. Boiko, V. Shendryk // Procedia Computer Science. 2017. Vol. 104. P. 35-42

15. Nazareth D.L. A system dynamics model for information security management / D.L. Nazareth, J. Choi // Information & Management. 2015. Vol. 52. № 1. P. 123 – 134

16. Herath H.S.B. IT security auditing: A performance evaluation decision model / H.S.B. Herath, T.C. Herath // Decision Support Systems. 2014. Vol. 57. IT security auditing. P. 54-63

17. The relationship between internal audit and infor-mation security: An exploratory investigation / Steinbart P.J., Raschke R.L., Gal G., Dilla W. N. // International Journal of Accounting Information Systems. 2012. Vol. 13.P. 228-243

18. ГОСТ Р ИСО/МЭК 15408-1-2008. Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий, 2008

19. Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации Классификация автоматизированных систем и требования по защите информации, 1992

20. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах: Приказ ФСТЭК №17 от 11 февраля 2013

Трапезников Евгений Валерьевич – старший преподаватель кафедры «Комплексная защита информации», ФГБОУ ВО ОмГТУ, тел. +7-913-673-94-76, e-mail:evtrapeznikov@yandex.ru.

DEVELOPMENT OF SOFTWARE FOR THE IMPLEMENTATION OF THE AUDIT PROCESS FOR CONTAINING INFORMATION SECURITY

E.V. Trapeznikov
Omsk State Technical University (OmSTU), Omsk

Abstract – The development of information processing and storage technologies leads to the emergence of new threats and vulnerabilities. To prevent the loss of information, both means of protection and regulatory framework are developed. Protective equipment used should provide the necessary level of protection. To confirm this level or notify about its shortcomings allows for a timely audit. The article deals with the development of software for the implementation of the process of auditing the protection system of automated systems. A developed model for assessing the security of information using intelligent tools is presented. A software algorithm was developed and implemented for auditing the state of security of an automated system for an information security specialist. The preliminary data for testing the developed algorithm and software package are given.

Index terms: audit, automated system, information properties, security management, information security model, MVC, ORM.

REFERENCES

1. *Information technology (IT). Methods and means of ensuring security. Code of norms and rules for information security management.,* Federal standard R ISO/IEC 27002-2012, Moscow, Standatrinform, 2014.

2. V.V. Salova and V.I. Vasiliev, *Intelligent decision support system for conducting audit of personal data information systems*, *Vestnik UGATU*, vol. 18, no. 3(64). pp. 261-269, 2014

3. S.A. Glushenko and A.I. Dolzhenko, *Decision support system for fuzzy modeling of information security risks of an organization*, *Informatsionnyye tekhnologii*, vol. 21, no. 1. pp. 68-74, 2015

4. S.I MakarenkoV., *Information security audit: the main stages, conceptual bases, classification of events*, *Sistemy upravleniya, svyazi i bezopasnosti*, no. 1, pp. 1-29, 2018.

5. D Dor. and Y. Elovici, *A model of the information security investment decision-making process.Computers&Security*, vol. 63. pp. 1-13, 2016

6. E.V. Trapeznikov, *Analysis of solutions for assessing the protection of information in information systems*, *Rossiya molodaya: peredovyye tekhnologii – v promyshlennost!*, no. 2. pp. 30-34, 2017

7. V.N. Maksimenko and Y E.V. Yasyuk, *The main approaches to the analysis and assessment of information security risks*, *Ekonomika i kachestvo sistem svya*, no. 2(4). pp. 42-48, 2017

8. A.A. Shelupanov *Actual directions of development of methods and means of protection of information*, *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki*, Vol. 20, no. 3. pp. 11-24, 2017

9. A.K. Novokhrestov, *A model of threats to the security of information and its carriers*, *Vestnik Irkutskogo gosudarstvennogo tekhnicheskogo universiteta*, Vol. 21, no. 12. pp. 30-34, 2017

10. P. J. Steinbart, *The influence of a good relationship between the internal audit and information security functions on information security outcomes*, In *Accounting, Organizations and Society*, 2018

11. Y.-C. Wei, Performance evaluation of the recommendation mechanism of information security risk identification, *Neurocomputing*, Vol. 279. pp. 48-53, 2018

12. H. Piech and G. Grodzki, *Audit expert system of communication security assessment.*, *Procedia Computer Science*, Vol. 112. pp. 147-156, 2017

13. D. Ki-Aries and S. Faily, *Persona-centred information security awareness*, In *Computers & Security*, Vol. 70. pp. 663-674, 2017

14. A. Boiko and V. Shendryk, *System Integration and Security of Information Systems*, *Procedia Computer Science, V*ol. 104. pp. 35-42, 2017

15. D.L. Nazareth, *A system dynamics model for information security management.*, In *Information & Management,* Vol. 52, no 1, pp. 123-134, 2015

16. H.S.B. Herath, *IT security auditing: A performance evaluation decision mode*, *Decision Support Systems*, Vol. 57. pp. 54-63, 2014

17. P.J. Steinbart, *The relationship between internal audit and information security: An exploratory investigation*, In *International Journal of Accounting Information Systems*, Vol. 13, pp. 228-243, 2012

18. *Information technology. Methods and means of security. Criteria for assessing the security of information technology*,Federal standard R ISO/IEC 15408-1-2008, Moscow, Standatrinform, 2014.

19. *Automated systems. Protection against unauthorized access to information Classification of automated systems and information security requirements,Guidance Document*, 1992.

20. *On the approval of requirements for the protection of information not constituting a state secret*, *Prikaz FSTEK №17, 11.02.2013*.

Trapeznikov Evgeny Valerievich – Senior Lecturer, Department of Integrated Protection of Information, Omsk State Technical University., +7-913-673-94-76, e-mail: evtrapeznikov@yandex.ru.