Вестник Сыктывкарского университета.
Серия 1: Математика. Механика. Информатика.
Выпуск 4 (29). 2018

УДК 378.147

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДЛЯ ПОДГОТОВКИ К ПРАКТИЧЕСКОМУ АУДИТУ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В. А. Воеводин, А. С. Заболотный, Э. О. Настинов

Рассмотрены особенности магистерской подготовки по программе «Аудит информационной безопасности автоматизированных систем», актуальность внедрения учебно-методического комплекса для организации деловой игры и приобретаемые при этом преимущества, подход к формализации объекта аудита. Сообщается о полученных результатах.
Ключевые слова: аудит, информационная безопасность, деловая игра.

В соответствии с правилами аудита, в том числе и аудита информационной безопасности (ИБ), аудитор должен изучить деятельность аудируемого лица [1; 2]. Особую актуальность это положение приобретает для объектов критической информационной структуры, для которых аудиторские ошибки из-за недостаточных знаний объекта аудита (ОА) могут нести потенциальную опасность, в том числе и катастрофическую. Отсюда следует, что аудиторы должны иметь соответствующую подготовку, которая должна быть объективно оценена до того, как они будут допущены к проведению аудита [2]. С этой целью в Московском институте электронной техники (МИЭТ) предусмотрена профессиональная подготовка по направлению 10.04.01 «Информационная безопасность» по программе магистратуры. Подготовка осуществляется в соответствии с Приказом Министерства образования и науки РФ от 1 декабря 2016 г. N 1513, которым был утверждён соответствующий Федеральный государственный образовательный стандарт высшего образования (ФГОС ВО). Программа подготовки магистров по направлению 10.04.01 в соответствии с ФГОС ВО ориентирована в том числе

на формирование способности решать следующие профессиональные задачи контрольно-аналитической деятельности: аудит информационной безопасности информационных систем и объектов информатизации; аттестация объектов информатизации по требованиям безопасности информации. В ФГОС ВО по направлению 10.04.01 предусмотрены требования по формированию *в том числе* компетенций по контрольно-аналитической деятельности: способности проводить аудит информационной безопасности информационных систем и объектов информатизации (ПК-9); способности проводить аттестацию объектов информатизации по требованиям безопасности информации (ПК-10).

С целью реализации названного ФГОС ВО на кафедре «Информационная безопасность» МИЭТ осуществляется подготовка магистрантов по специальности «Аудит информационной безопасности автоматизированных систем». В рамках подготовки формируется базисный задел для дальнейшей профессиональной деятельности по специальности.

В соответствии с программой магистерской подготовки «Аудит информационной безопасности автоматизированных систем» по направлению 10.04.01 «Информационная безопасность» (Программа) выпускники должны приобрести компетенции, которые можно сформировать лишь в том случае, если в учебный процесс будут внедрены задачи практического аудита, актуальные для реального объекта аудита (ОА) или максимально приближенные к реальному. С этой целью на завершающем этапе обучения (четвертый семестр) Программой предусмотрено проведение деловой игры (ДИ), в ходе которой решаются отдельные аудиторские задачи и осуществляется оценка готовности участников ДИ к проведению аудита. Однако увязать их в единый комплекс с признаками полноценного практического аудита не представляется возможным из-за недостаточных производственных возможностей учебного оборудования, отсутствия доступа к испытательным стендам для построения среды виртуализации реального ОА, которыми в комплексе обладают предприятия, на которых магистранты проходят производственную практику и стажировку.

Для понимания сути проблемы аудита следует мысленно встать на философские позиции и увидеть две категории: а) истинное состояние ОА и б) эмпирическое (опытное) проявление этого состояния в результатах аудиторских наблюдений, на основании которых аудитор выводит суждение об истинном состоянии ОА. Истинное состояние аудитор желает познать посредством количественных и качественных наблюдений за свойствами (характеристиками) данного объекта, и оно для аудитора является идеальным (неизвестным). Истинное состояние объекта

аудита не зависит ни от средств наблюдения, ни от познаний самого аудитора и является для него абсолютной истиной, которую он желает познать.

Результаты аудиторских наблюдений, напротив, являются продуктами познания объекта аудита, представляя собой лишь оценки наблюдаемых свойств, найденные путем наблюдения, они зависят не только от самого аудитора, но еще и от метода наблюдения за соответствующим свойством, от технических средств, с помощью которых проводится наблюдение, и методов обработки результатов аудиторских наблюдений.

Разница между результатами измерений, полученных при наблюдении за тем или иным свойством ОА, и его истинным значением измеряемой (наблюдаемой) величины характеризует погрешность наблюдения (измерения), что определяет аудиторский риск.

Анализ литературы по организации обучения, в том числе и в сетевой форме [6; 7; 9; 10], позволил выдвинуть гипотезу, что для формирования компетенций по проведению практического аудита ИБ наиболее подходит подготовка в форме деловой игры.

Анализ литературы по организации деловых игр [4; 5; 9; 11] в других областях, особенностей объекта аудита, технологий организации аудита, требований к компетенции выпускника позволяет утверждать, что необходим образовательный продукт, поддерживающий организацию и проведение ДИ в виде учебно-методического комплекса (УМК), состоящий из отдельных образовательных модулей, объединенных единой целью, с возможностью построения среды виртуализации информационной и организационной инфраструктуры и настройки её под конкретный ОА. Важным требованием к УМК является возможность реализации сетевой формы обучения, которая ориентирована на использование ресурсов нескольких организаций: образовательных, научных, производственных. Данный подход позволит значительно снизить стоимость владения УМК, так, потребность в этом ресурсе возникает периодически и на относительно короткое время — в нашем случае это четвертый семестр магистратуры на 72 часа, в остальное время УМК будет просто простаивать.

Анализ аудита информационной безопасности (АИБ) как технологического процесса [2; 3] позволил принять гипотезу, что задача аудита, в том числе и АИБ, имеет относительно самостоятельное значение. Это утверждение было принято исходя из *принципа внешнего дополнения*, который является фундаментальной идеей теории систем [7]. Принятие внешнего дополнения [8] позволило преодолеть геделевскую трудность и ограничить изучаемый процесс рамками предмета исследования; вы-

членить из процесса обеспечения ИБ как метапроцесса некую целостность — подсистему АИБ, выдвинуть гипотезы поведения субъектов АИБ и перейти к формализованному описанию аудита на уровне «организация — поведение». Кроме того, *внешнее дополнение* позволило согласовать цель обеспечения ИБ с целью АИБ и задать мотивированные требования к УМК.

Для построения УМК ОА был формально определен как система (1), представляющая собой множество *наблюдаемых* свойств — $\{a_i\}$, с каждым из которого связано множество его *проявлений* — $\{A_i\}$ и множество *варьируемых* свойств — $\{b_i\}$, с каждым из которого связано множество его *изменений* — $\{B_i\}$.

$$\mathbf{OA} = (\{a_i, A_i), i \in N_n\},\ (\{b_i, B_i), i \in N_m\}, \tag{1}$$

где $N_n = \{1, 2, \ldots, n\}$ — значение индекса наблюдаемого свойства, n — число наблюдаемых свойств, $N_m = \{1, 2, \ldots, m\}$ — значение индекса варьируемого свойства, m — число варьируемых свойств.

Во многих случаях множества $\{A_i\}$ неизвестны и могут быть получены либо опытным путем, либо на основании философских построений.

Далее в УМК был введен новый элемент — канал наблюдения [8], под которым понимается операция, вводящая конкретную переменную как образ того или иного наблюдаемого свойства ОА. Канал наблюдения был реализован с помощью функции (2):

$$o_i : A_i \longrightarrow V_i. \tag{2}$$

Считается, что эта функция гомоморфна относительно предполагаемых свойств множеств A_i и V_i, где V_i — множество возможных значений переменной, с помощью которой отражаются соответствующие свойства ОА, принадлежащие множеству A_i.

Для обоснования структуры УМК, его декомпозиции в соответствии с методическими уровнями была принята исходная парадигма УМК. Обобщенная модель архитектуры УМК приведена на рис. 1. УМК был представлен как сферическая четырехуровневая схема соответствующих методических уровней:

первый — аудиторского заключения;

второй — аудиторских доказательств;

третий — аудиторских свидетельств;

четвертый — наблюдаемых свойств объекта аудита.

Методические уровни разделены между собой межуровневыми интерфейсами, представляющими собой методические фильтры Ф. Мето-

дические фильтры УМК построены от общего к частному:

Фильтр Φ_0 позволяет отобразить задачу аудита в требования к содержанию аудиторского заключения (АЗ);

Φ_1 — требования к содержанию аудиторского заключения – в требуемое множество аудиторских доказательств (АД) $\{\text{ад}_i\}$, где i — мощность множества;

Φ_2 — требования к содержанию соответствующего аудиторского доказательства – в требуемое множество аудиторских свидетельств (АС) $\{\text{ас}_j\}_i$, где j — мощность множества, i — индекс аудиторского доказательства;

Φ_3 — требования к содержанию аудиторского свидетельства — в требуемое множество наблюдаемых свойств (НС) $\{\{\text{as}_k\}_j\}_i$, где k — мощность множества наблюдаемых свойств, j — индекс аудиторского наблюдения, i — индекс аудиторского доказательства.

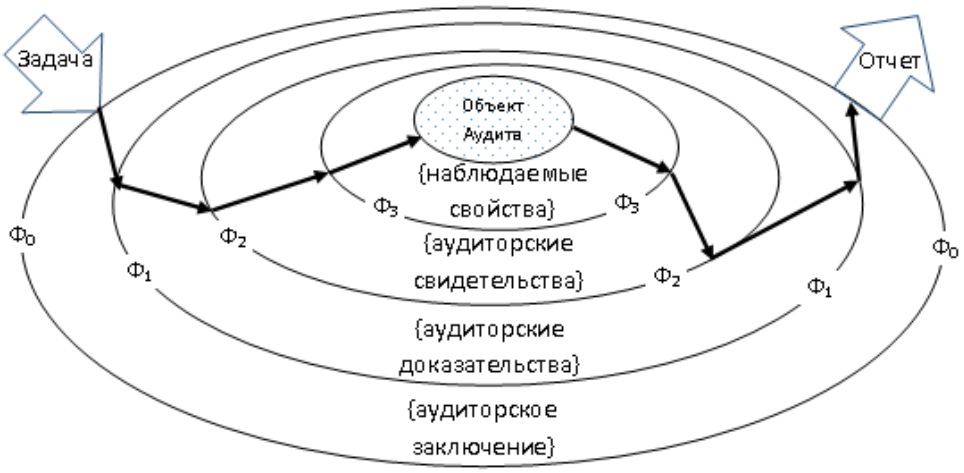

Рис. 1. Обобщенная модель архитектуры УМК

После того как все фильтры настроены, считается, что УМК настроен под особенности конкретного объекта аудита и можно приступать к разработке программы АИБ и планированию аудита.

Реализация программы и плана аудита осуществляется от частного к общему:

– с помощью настроенного фильтра Φ_3 осуществляется отображение измеренных показателей наблюдаемых свойств в соответствующее множество аудиторских свидетельств;

– с помощью Φ_2 — множество добытых аудиторских свидетельств – в соответствующее аудиторское доказательство;

– с помощью Φ_1 — множество аудиторских доказательств – в аудиторское заключение;

– с помощью Φ_0 осуществляется преобразование аудиторского заключения в аудиторский отчет и осуществляется интерпретация полученного результата аудита в форму, понятную лицу, принимающему решение.

Таким образом, УМК разбивается на четыре методических уровня, для каждого уровня строится своя модель, а взаимодействие между уровнями осуществляется через соответствующий интерфейс. Причем технология обработки данных каждого из уровней скрыта от смежных уровней, реализован принцип инкапсуляции. Принятие данного принципа позволяет снизить сложность УМК.

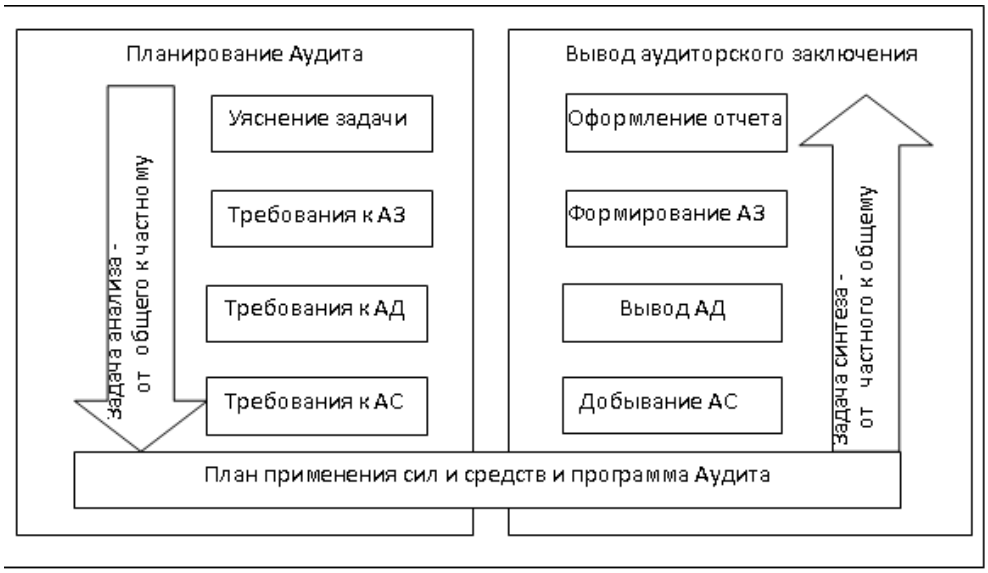

Рис. 2. Иерархическая классификация задач УМК

С помощью декомпозиции УМК по методическим уровням была разработана иерархическая классификация задач аудита, составляющих его организационную основу. Иерархическая классификация приведена на рис. 2.

При построении иерархии задач УМК принят принцип внешнего дополнения и принцип инкапсуляции [8], в соответствии с которым при настройке УМК задачи верхнего уровня предоставляют исходные данные для задач нижнего уровня, а при выводе аудиторского заключения результаты решения задач нижнего уровня являются исходными данными для задач верхнего уровня. Причем содержание методики решения

задач каждого из методических уровней скрыта от смежных уровней, взаимодействие уровней осуществляется через соответствующий методический интерфейс.

Анализ форм и способов подготовки аудиторов, проведенный авторским коллективом [2; 3], позволяет еще раз подтвердить, что эффективным способом подготовки аудиторов является деловая игра (ДИ), которая позволит: обучать аудиторов на ситуационных задачах, приближенных к реальным; осуществлять объективную оценку подготовки аудиторов, тем самым снижая аудиторский риск; реализовать сетевую технологию обучения, тем самым снижая стоимость владения УМК.

Для разработки УМК в целях проведения практического АИБ в инициативном порядке был открыт проект «Учебно-методический комплекс по подготовке к практическому аудиту» (далее — Проект). Реализация Проекта запланирована в три этапа: первый — разработка среды виртуализации документационного обеспечения ИБ (разработаны учебные политики и регламенты). Первый этап завершен в июне 2018 г. Второй — проведение научно-исследовательских изысканий по моделированию ОА, разработке соответствующего методического обеспечения — продолжается на настоящий момент. Завершение — июнь 2019 г. Третий — реализация результатов научно-исследовательских изысканий, сетевой технологии обучения. Срок завершения — июнь 2020 г. Первые два этапа не требовали финансирования и выполнялись силами студентов, в основном выпускниками магистратуры. Третий этап требует финансирования, поэтому принято решение по участию в конкурсе на получение гранта.

Что касается учебного процесса, то внедрение УМК позволит повысить эффективность подготовки магистрантов к практическому аудиту, сформировать дополнительные актуальные компетенции, которые востребованы программой цифровой экономики и в явном виде не отражены в ФГОС ВО:

1. Способность осуществлять календарное и ресурсное планирование применения сил и средств аудита ИБ с использованием специализированного программного обеспечения.

2. Способность разрабатывать имитационные модели объекта аудита, игровые модели аудиторских операций, планировать эксперимент с ними и применять полученные результаты для разработки программы и плана аудита ИБ.

3. Способность применять апробированные методы проектного управления для организации аудита ИБ.

4. Способность адаптировать проверенные на практике методы и

приемы аудита достоверности финансовой отчетности для целей аудита ИБ.

5. Способность формулировать требования к сценарию ДИ и базе знаний по предметной области.

Положительный эффект от внедрения УМК заключается в том, что он имеет не только ценность для организации учебного процесса, но и реальную коммерческую ценность для организации практического аудита, а также для формирования стандартов аудиторской деятельности. Наличие стандартов аудиторской деятельности является необходимым условием, чтобы таковая была признана аудитом [1].

Результаты проекта жизнеспособны и имеют устойчивый результат, так как базируются на апробированном теоретическом фундаменте и на опыте проведения аудита в смежных областях.

Полученные результаты регулярно докладываются участниками Проекта на профильных конференциях и публикуются в специализированных изданиях.

В чем заключается методологическая и содержательная новизна применения УМК для проведения ДИ?

Традиционный подход базируется на системе лекционных и практических форм обучения и традиционных формах оценки компетенций, которые нацелены на формирование знаний, умений, навыков, применение которых отнесено как минимум на начало профессиональной деятельности.

Деловая же игра базируется на поиске и обобщении знаний, которые непосредственно требуются «здесь и сейчас» для решения поставленных ситуационных задач (кейсов). Набор знаний, умений и навыков адаптируется к игровой ситуации, что повышает мотивацию обучающегося. Более того, в результате деловой игры формируется базовый набор решений практических задач, который может быть использован выпускником как методический задел для начала профессиональной деятельности.

Востребованность вузовским и образовательным сообществом определяется тем, что аудит ИБ как предмет обучения является трудноформализуемым и на текущий момент не имеет достаточной теоретической проработки. В связи с этим аудиторы применяют методическое обеспечение собственной разработки, что отрицательно сказывается на доверии к аудиторскому заключению заинтересованных сторон. Применение УМК позволит выработать задел для стандартизации аудиторских операций.

Деловая игра по традиционному сценарию (без применения УМК)

проводилась уже два раза, поэтому имеется определенный методический задел: накоплен методический задел, касающийся организационного обеспечения экспертного аудита ИБ; разработаны учебные политики и регламенты по обеспечению ИБ, которые служат объектом экспертного аудита; разработаны методические рекомендации по применению отельных инструментальных средств аудита; обобщены полученные за этот период эмпирические знания, позволяющие обосновать дидактические требования к УМК; усовершенствованы сценарий проведения ДИ и образовательные технологии. Результаты первого этапа будут апробированы уже в следующем году при проведении ДИ.

Результаты разработки УМК докладывались участниками Проекта на двух конференциях:

1. Национальная (Всероссийская) научная конференция «Математическое моделирование и информационные технологии», проводимая в г. Сыктывкар в декабре 2018 года (http://mmit2018.syktsu.ru/) по следующим вопросам:

1. Деловая игра. Учебно-методический комплекс для подготовки к аудиту.

2. О модели объекта аудита информационной безопасности.

2. Российская научная конференция «Интеллектуальные системы в информационном противоборстве» в декабре 2018 года (http://analyticswar.ru/p%D1%81ommittee/) по следующим вопросам:

• о подготовке аудиторов информационной безопасности к практическому аудиту в форме деловой игры;

• об оценке значимости аудиторских свидетельств;

• об оценке готовности аудиторской группы к проведению практического аудита;

• о подготовке программы аудита информационной безопасности;

• об игровой модели деловой игры аудита информационной безопасности;

• о моделировании информационной инфраструктуры объекта аудита с применением технологий виртуализации.

Подготовлены материалы по результатам выступлений для публикации в соответствующем рецензируемом сборнике конференции.

Образовательный продукт в форме УМК планируется внедрить в апреле 2020 года.

Список литературы

1. Об аудиторской деятельности : федеральный закон от 30.12.2008 N 307-ФЗ (ред. от 23.04.2018). Ст. 1, п. 2.

2. ГОСТ Р ИСО/МЭК 27006-2006. Информационная технология. Методы и средства обеспечения безопасности. Требования к органам, осуществляющим аудит и сертификацию систем менеджмента информационной безопасности. Введ. 2008-18-12 №524-ст. М.: Стандартинформ, 2010. 35 с.

3. ГОСТ Р ИСО/МЭК 27004-2012. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения. Введ. 2011-01-12 №681-ст. М.: Стандартинформ, 2012. 55 с.

4. **Абрамова Г. С., Степанович В. А.** Деловые игры: теория и организация. Екатеринбург: Деловая книга, 1999. 192 с.

5. **Айламазьян А. М.** Актуальные методы воспитания и обучения: деловая игра. М.: Владос-пресс, 2000. 332 с.

6. **Дьюи Дж.** Образование консервативное и прогрессивное // Демократия и образование : пер. с англ. М.: Педагогика-Пресс, 2000. 384 с.

7. **Корнели Д., Данофф Ч.** Парагогика: синергия самостоятельной и организованной учебной деятельности / пер. И. Травкина // *Проблемы управления в социальных системах. 2014. Т. 7. Вып. 11. С. 84–97.*

8. **Клир Дж.** Системология. Автоматизация решения системных задач. М.: Радио и связь, 1990. 544 с.

9. **Панфилова А. П.** Игротехнический менеджмент. Интерактивные технологии для обучения и организационного развития персонала : учебное пособие. СПб.: ИВЭСЭП, 2003. 536 с.

10. **Патаракин Е. Д.** Социальные взаимодействия и сетевое обучение 2.0. М.: НП «Современные технологии в образовании и культуре», 2009. 176 с. С. 34.

11. **Платов В. Я.** Деловые игры: разработка, организация и проведение : учебник. М.: Профиздат, 1991. 156 с.

Summary

Voevodin V. A., Zabolotni A. S., Nastinovn E. O. Training complex to prepare for the practical security audit

The features of master's training in the program «Audit of information security of automated systems», the relevance of the implementation of educational and methodical complex for the organization of business games and the acquired advantages, the approach to the formalization of the object of audit. The results are reported.

Keywords: audit, information security, business game.

References

1. *Federal'nyy zakon ot 30.12.2008 N 307-FZ (red. ot 23.04.2018) «Ob auditorskoy deyatel'nosti»* (Federal law of 30.12.2008 N 307-FZ (as amended on 04.23.2018) «On Auditing »), Art. 1, p. 2.

2. *GOST R ISO/MEK 27006-2006. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Trebovaniya k organam, osushchestvlyayushchim audit i sertifikatsiyu sistem menedzhmenta informatsionnoy bezopasnosti* (GOST R ISO / IEC 27006-2006. Information technology. Methods and means of security. Requirements for bodies performing the audit and certification of information security management systems), Enter 2008-18-12, No. 524-st, Moscow: Standardinform Publ., 2010, 35 p.

3. *GOST R ISO/MEK 27004-2012. Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment informatsionnoy bezopasnosti* (GOST R ISO / IEC 27004-2012. Information technology. Methods and means of security. Information Security Management. Measurements), Enter 2011-01-12 № 681-ст, Moscow: Standardinform Publ., 2012, 55 p.

4. **Abramova G. S., Stepanovich V. A.** *Delovyye igry: teoriya i organizatsiya* (Business games: theory and organization), Ekaterinburg: Business book Publ., 1999, 192 p.

5. **Aylamazyan A. M.** *Aktual'nyye metody vospitaniya i obucheniya: delovaya igra* (Actual methods of education and training: a business game), Moscow: Vlados - press Publ., 2000, 332 p.

6. **Dewey J.** *Obrazovaniye konservativnoye i progressivnoye / Demokratiya i obrazovaniye* (Conservative and progressive education /

Democracy and education), Moscow: Pedagogy Press Publ., 2000, 384 p.

7. **Corneli D., Danoff Ch.** Paragogika: sinergiya samostoyatel'noy i organizovannoy uchebnoy deyatel'nosti (Paragogik: Synergy of Independent and Organized Learning Activities), Per. I, Travkina, *Management problems in social systems*, 2014, t. 7, vol. 11, pp. 84–97.

8. **Clear J.** *Sistemologiya. Avtomatizatsiya resheniya sistemnykh zadach* (Systematology. Automation of solving system problems), Moscow: Radio and communication Publ., 1990, 544 p.

9. **Panfilova A. P.** *Igrotekhnicheskiy menedzhment. Interaktivnyye tekhnologii dlya obucheniya i organizatsionnogo razvitiya personala* (Igrotechnical management. Interactive technologies for staff training and organizational development), Tutorial, SPb IVESEP, 2003, 536 p.

10. **Patarakin E.** *Sotsial'nyye vzaimodeystviya i setevoye obucheniye 2.0* (Social Interactions and Networked Learning 2.0), Moscow: NP «Modern technologies in education and culture», 2009, 176 p.

11. **Platov V. Ya.** *Delovyye igry: razrabotka, organizatsiya i provedeniye* (Business games: development, organization and implementation: Textbook), Moscow: Profizdat Publ., 1991, 156 p.

Для цитирования: Воеводин В. А., Заболотный А. С., Настинов Э. О. Учебно-методический комплекс для подготовки к практическому аудиту информационной безопасности // *Вестник Сыктывкарского университета. Сер. 1: Математика. Механика. Информатика. 2018. Вып. 4 (29). С. 60–71.*

For citation: Voevodin V. A., Zabolotni A. S., Nastinovn E. O. Training complex to prepare for the practical security audit, *Bulletin of Syktyvkar University. Series 1: Mathematics. Mechanics. Informatics*, 2018, 4 (29), pp. 60–71.

Национальный исследовательский университет «МИЭТ»

Поступила 10.01.2019