ОРИГИНАЛЬНАЯ СТАТЬЯ

DOI: 10.26794/2408-9303-2019-6-6-24-33
УДК 378.1:004.056(045)
JEL D83, M15, M42, H83

О концепции проведения аудита информационной безопасности в вузе

В.Н. Ясенев[a], А.В. Дорожкин[b], А.Л. Сочков[c]
Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, Россия
[a] https://orcid.org/0000-0003-0306-2680; [b] https://orcid.org/0000-0003-3578-6421;
[c] https://orcid.org/0000-0001-8389-9493

АННОТАЦИЯ

В статье рассмотрены теоретические и практические основы аудита информационной безопасности (ИБ) образовательных учреждений, высказаны предложения по основным составляющим его концепции с учетом специфики учебных организаций, проведен поиск путей обеспечения эффективного функционирования вузов. Методологической основой исследования явилась система анализа и синтеза подходов к проведению внутреннего аудита ИБ. Сделаны предложения по разработке проекта комплексной концепции проведения аудита ИБ вуза, включающей семь составляющих: объекты аудита; его цели и задачи; подвид аудита, учитывающий особенности учебного заведения; подходы к проведению аудита и методы анализа данных, полученных в процессе проверки; этапность аудита; его организационно-технические основы; состав и содержание результирующих документов. Рекомендована к применению комбинация анализа рисков и стандартов в области ИБ, а также экспериментальное изучение системы безопасности объектов для ее реальной проверки. Среди оснований теоретических подходов, которые могли бы создать базу для аудита ИБ высшего учебного заведения, предпочтительно выглядят модели оценки и «серого» ящика. Практическая реализация предложенной концепции аудита ИБ позволит повысить эффективность мониторинга исполнения федеральных законов и программ в образовательном заведении, усилить уровень ИБ организации.

Ключевые слова: высшее учебное заведение; информационная безопасность; аудит информационной безопасности; этапы аудита; риски и стандарты; документы

Для цитирования: **Ясенев В.Н., Дорожкин А.В., Сочков А.Л. О концепции проведения аудита информационной безопасности в вузе. *Учет. Анализ. Аудит.* 2019;6(6):24-33. DOI: 10.26794/2408-9303-2019-6-6-24-33**

ORIGINAL PAPER

Draft Concept of Information Security Auditing at a University

V.N. Yasenev[a], A.V. Dorozhkin[b], A.L. Sochkov[c]
Lobachevsky State University of Nizhny Novgorod, Nizhny Novgorod, Russia
[a] https://orcid.org/0000-0003-0306-2680; [b] https://orcid.org/0000-0003-3578-6421;
[c] https://orcid.org/0000-0001-8389-9493

ABSTRACT

The article examines the theoretical and practical basis of auditing the information security of educational institutions. The article gives proposals on the main components of its concept, taking into account the specifics of educational organizations, the article also searches for the ways of ensuring the effective functioning of universities on a considered basis. Proposals have been made to develop a comprehensive concept for the auditing of the information security of the university. The project includes seven components: the objects of auditing; its goals and objectives; the subtype of auditing that takes into account the specifics of the school; how to conduct audits and how to analyze data from the auditing process; the auditing phasing; its organizational and technical foundations; the composition and content of the resulting documents. A combination of risk analysis and information security standards is recommended as a practical approach to auditing. It is recommended that an experimental examination of the object security system should be

used for real verification. Among the reasons for theoretical approaches that could create the basis for auditing the information security of a higher educational institution, the most preferable are the models of evaluation and the "grey" box. Practical implementation of the proposed information security auditing concept will improve the effectiveness of monitoring the implementation of Federal Laws and Programs in the educational institutions, and it will eventually strengthen the level of information security of the organization.
Keywords: university; information security; information security auditing; audit stages; risks and standards; documents

For citation: **Yasenev V.N., Dorozhkin A.V., Sochkov A.L. Draft concept of information security auditing at a university. *Uchet. Analiz. Audit* = *Accounting. Analysis. Auditing.* 2019;6(6):24-33. (In Russ.). DOI: 10.26794/2408-9303-2019-6-6-24-33**

ВВЕДЕНИЕ

Развитие страны в рамках национальной программы «Цифровая экономика Российской Федерации»[1] обусловливает и активное внедрение информационных технологий в вузах, повышающих эффективность образовательных, научно-исследовательских процессов и управленческой деятельности. Модель цифрового университета предполагает гармоничное сочетание современных методологических подходов и инновационных цифровых технологических решений. Появление в организациях высшего образования новых информационных ресурсов и сервисов (многофункциональные интернет-порталы, компьютерные классы, широкополосный интернет и локальные сети, интерактивные обучающие курсы и т.д.) увеличивает риск возникновения инцидентов информационной безопасности (ИБ), реальные последствия которых могут снижать эффективность работы вуза.

Сегодня у руководства большинства высших учебных заведений нет сомнений в необходимости серьезно заботиться об информационной безопасности в организации (сохранение информации о работе вуза, учащихся, преподавателях, обеспечение целостности и сохранности электронных документов и т.д.), поскольку отмеченная национальная программа акцентирует на этом внимание. Одним из важнейших факторов эффективного функционирования современного учреждения высшего образования является комплексная система ИБ, ключевым элементом которой является перманентный аудит.

В настоящее время проблемы усиления безопасности информационных данных вуза рассматриваются специалистами нескольких областей знаний, поскольку такие работы требуют одновременной компетентности исследователей как в аудите, так и в современных информационных системах и технологиях.

Исследованием разнообразных аспектов информационной безопасности предприятий и учреждений занимаются многие ученые и специалисты: В.И. Завгородний, А.Ф. Беззубов, Е.В. Боякова, А.И. Козачок, А.П. Курило, Ю.А. Левицкая, Н.Н. Панов, В.П. Поляков, О.В. Стукалова, И.В. Синицын, А.В. Тюменев, А.А. Шабанов, О.В. Юдушкина, В.Н. Ясенев и др. В то же время при многоаспектности и обширности таких исследований еще недостаточно теоретических исследований и практических предложений по учреждениям сферы высшего образования.

В работе В.И. Завгороднего [1] проведен всесторонний анализ состава вычислительного и сетевого оборудования с позиций их защищенности, в публикации А.Ф. Беззубова и И.В. Синицына [2] — анализ информационных угроз, связанных с применением в образовательном учреждении ведомственного подчинения зарубежной техники и компьютерных программ. Совершенно справедливы предложения авторов о внедрении отечественных аппаратных и программных средств для исключения отмеченных угроз и повышения уровня защищенности ресурсов, однако экономические аспекты и проблемы аудита ими не затронуты.

А.И. Козачок, Ю.А. Левицкая [3], рассматривая методы оценки информационных рисков для компьютерных сетей учебного заведения, предлагают использовать табличную методику анализа ввиду ее простоты и наглядности, однако сам аудит ИБ подобных сетей, как мероприятие повышения уровня их защищенности, обходят стороной.

Работа [4] посвящена вопросам информационной безопасности вузов в сфере культуры и искусства. Авторы рекомендуют применять системный подход к решению изучаемых проблем, однако, ИБ ими трактуется в узком смысле, прежде всего как

[1] Указ Президента РФ № 204 от 07.05.2018 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года». URL: http://prezident.org/articles/ukaz-prezidenta-rf-204-ot-7-maja-2018-goda-07–05–2018.html (дата обращения: 03.06.2019).

защита компьютерных сетей учебных учреждений. Аудит ИБ также не является элементом предлагаемой системы.

Исследование [5] делает упор на комплексный подход к информационной безопасности вуза. В нем анализируются особенности образовательных заведений с точки зрения построения системы защиты данных, однако в комплексе мероприятий по повышению уровня противодействия различным угрозам аудит ИБ отсутствует.

В статье А. А. Шабанова выявлены предпосылки создания системы ИБ в учебных организациях, определена нормативно-правовая база, озвучены этапы ее реализации, среди которых отмечен и аудит системы менеджмента информационной безопасности (СМИБ). Содержание понятия аудита ИБ, как и наполнение этого этапа, мероприятиями в работе не обозначено, кроме этого, процесс создания СМИБ опирается на международные стандарты, хотя в РФ они адаптированы к российской действительности и реализованы в виде ГОСТов на момент публикации статьи [6].

Изучению вопросов аудита ИБ посвящены работы [7–12]. В них рассмотрены цели и задачи, виды, этапы и мероприятия аудита, основные подходы и принципы, используемые при планировании и реализации процесса, однако их исследовательские наработки нельзя применить без модернизации для осуществления вузовского аудита, поскольку здесь имеют место специфические особенности учебного заведения, отличающие его от любого другого объекта ИБ. Исследований, посвященных непосредственно наполнению аудита ИБ образовательного учреждения, обнаружить не удалось.

В [7, 8] сформулированы цели и место аудита информационной безопасности в общей системе ИБ экономического субъекта, отмечена эффективность применения комплексного и системного подхода к его воплощению в жизнь. В работах выделена мысль, что специфика конкретного объекта аудита влияет и определяет цели, задачи, виды и этапы предстоящего действия. Также проанализированы и сопоставлены часто встречающиеся подходы анализа данных, собираемых аудитором в процессе исполнения договора. Вместе с тем в этих исследованиях не разбираются нюансы разнообразных подвидов аудита ИБ и условия их применимости к различным экономическим субъектам, таким образом, остается открытым вопрос о типе действия, применимом к конкретному объекту аудита.

В [9] отмечается отсутствие единого стандарта и единой методики по аудиту ИБ в РФ, предпринята попытка разработки его концептуальных основ для применения в органах внутренних дел. Предложены принципы осуществления аудита, сформулированы цели и направления процесса по шагам или этапам, сформирован комплекс организационных мероприятий. В этой работе дан анализ применимости подвидов аудита ИБ для органов внутренних дел с акцентом на внешний независимый тип, но для вузов в условиях их ограниченного финансирования этот вариант пока представляется малоперспективным и предпочтительнее выглядит аудит внутренний.

В [10] исследуется внутренний аудит информационной безопасности предприятия, но рассмотрение концентрируется только на проверку учетно-информационной системы экономического субъекта. Дано обоснование данного подвида, но без упора на финансовую составляющую мероприятий. Основные предложенные этапы процесса базируются на международном стандарте серии ISO/IEC 27000[2], хотя на момент публикации работы уже появились отечественные адаптированные аналоги этой линейки.

Работа [11] представляется наиболее продвинутым и фундаментальным исследованием в рассматриваемом секторе. В ней уточняются понятие аудита ИБ, варианты целей и задач для него, состав его основных этапов. Особое внимание сфокусировано на концепции, которая подразумевает идентификацию моделей угроз, соперников и самого аудита, а также основные теоретический и практический подходы к его реализации. В статье приводится типология существующих мероприятий аудита и критерии их классификации, однако не даются рекомендации по их применению к конкретно взятым экономическим субъектам.

Таким образом, целью данной статьи выступает изучение теоретических и практических основ аудита ИБ образовательных учреждений, предложение и обсуждение отдельных основных составляющих его концепции с учетом специфики учебных организаций, а также поиск путей обеспечения эффективного функционирования вузов на рассмотренной основе.

---

[2] Общие сведения о стандартах серии ISO 27000. URL: http://iso27000.ru/standarty/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu-1/iso-27000-mezhdunarodnye-standarty-upravleniya-informacionnoi-bezopasnostyu (дата обращения: 27.05.2019).

КОНЦЕПТУАЛЬНЫЕ СОСТАВЛЯЮЩИЕ АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВУЗА

Традиционная аудиторская деятельность в РФ регулируется рядом нормативных документов, например Федеральным законом от 30.12.2008 № 307-ФЗ «Об аудиторской деятельности». Ее целью является проверка финансовой отчетности организации и консультационные услуги, однако при этом существует объективная необходимость правового сопровождения и аудита ИБ при сохранении традиционных принципов (независимость проверки, наличие квалификационного аттестата аудитора, его деловая репутация, обязанность хранить тайну проверяемых организаций). В процессе осуществления аудиторской проверки ИБ вуза целесообразно также проверять выполнение таких правовых документов, как:

- Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ;
- Федеральный закон «Об электронной подписи» от 06.04.2011 № 63-ФЗ;
- Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».

Для проведения аудита ИБ вуза необходимо использовать комплексную концепцию, проект которой представлен в данной статье. Основные ее составляющие следующие:

- идентификация объектов проверки;
- цели и задачи проверки;
- предпочтительный подвид проверки;
- рекомендуемые подходы к проведению проверки и методы анализа данных;
- этапность проведения проверки;
- организационно-технические основы аудиторской проверки;
- состав результатов аудита.

Для целостного восприятия структура предлагаемой концепции представлена графически (*рис. 1*). В основе процесса лежит идентификация объектов аудита, относительно которых определяются цели и задачи проверки. Опираясь на них, выбирается оптимальный подвид аудита, который будет базироваться на теоретическом и практическом подходах к проведению проверки. Далее фиксируются этапность и сроки проведения аудита, а также его организационно-технические основы. Состав результатов проверки логически завершает пирамиду процесса.

Рис. 1 / Fig. 1. **Структура концепции проведения аудита информационной безопасности вуза / The concept structure of the information security auditing at a university**

Источник / Source: разработано авторами / developed by the authors.

Далее предлагается и обсуждается конкретное содержательное наполнение сформулированных авторами элементов концепции.

1. Идентификация объектов аудиторской проверки ИБ вуза. Принципиальной особенностью образовательных учреждений с точки зрения ИБ является необходимость обеспечения безопасности разнообразных данных в разворачиваемых компьютерных сетях [4], поэтому принципиальным объектом представляется информационная система образовательного заведения, базирующаяся на сетях такого рода.

В качестве идентифицируемых объектов отмечаем информационно-образовательные процессы в вузе, в ходе которых обучающиеся, получив задание преподавателя, самостоятельно разыскивают материал по теме, используя ресурсы сети Интернет. Предполагается, что полученные сведения составят базу знаний студентов, однако добытая таким образом информация нередко на поверку оказывается недостоверной. Такой результат приводит к снижению эффективности формирования компетенций учащихся, что не может не беспокоить. Таким образом, познавательные процессы необходимо подвергать аудиторской проверке, поскольку они напрямую формируют менталитет выпускника вуза.

2. Цели и задачи информационного аудита вуза. Основные цели аудита ИБ образовательного уч-

реждения можно сформулировать следующим образом:

• выявление и детальное изучение угроз ИБ и «слабых звеньев» активов объектов аудита;

• определение набора мероприятий для повышения уровня безопасности системы защиты активов объектов аудита;

• создание таких условий функционирования объектов аудита, при которых реализация инцидентов ИБ была бы невозможна.

Основной задачей информационного аудита вуза является контроль и оценка объектов аудита на соответствие требованиям к уровню их информационной безопасности. Вспомогательными задачами могут являться:

• определение уровня актуальной защищенности объектов;

• идентификация «слабых» и «узких» мест в системе защиты объектов;

• оценка рисков, обусловленных возможным воплощением в реальность информационных угроз;

• определение уровня, насколько изучаемые объекты и система их защиты соответствует требованиям норм по информационной безопасности и положениям документа о политике безопасности учебного заведения;

• подготовка пакета рекомендаций для эффективного функционирования актуальной системы ИБ вуза и ее последующей модернизации.

3. Предпочтительный тип аудита для вуза. При обсуждении проблемы выбора наиболее адекватного подвида аудита ИБ будем руководствоваться терминологией и классификацией, приведенными в работе [11].

В первую очередь проанализируем подразделение по положению специалиста относительно проверяемого объекта, которое определяет внешний и внутренний аудит.

В процессе проектирования комплекса мер аудита ИС вуза важно понимать состояние защищенности ценных ресурсов, чтобы противостоять внешним и внутренним угрозам ее безопасности. Поиск путей решения проблем должен осуществляться не только силами самого вуза, но и при помощи внешних консультантов, в частности аудиторов. Поэтому реальную помощь может оказать независимое аудиторское исследование. В то же время при проведении такого аудита специалисты сталкиваются с проблемой сопоставления возможных расходов на обеспечение безопасности и выгод, получаемых при внедрении системы ИБ, поэтому в условиях ограниченного финансирования высшей школы не менее перспективным выглядит внутренний тип аудита образовательного учреждения, позволяющий использовать квалифицированный кадровый контингент вуза при меньших затратах.

Аудит безопасности деятельности вуза в сфере информационных технологий целесообразно проводить экспертным путем. При его проведении выявляются недостатки в системе мер защиты информации на основе опыта экспертов, участвующих в аудите. Цель проведения экспертного аудита — оценка состояния ИС, других объектов и разработка рекомендаций по применению комплекса организационных мероприятий и программно-технических средств, направленных на защиту ресурсов объектов аудита от угроз. Подобного типа аудит позволяет принять обоснованные решения по использованию средств защиты, оптимальных по их стоимости и возможности предотвращения угроз информационной безопасности в вузах. Такой аудит может базироваться на анализе риска. Опираясь на методы анализа риска, специалист определяет для обследуемой ИС и других объектов аудита индивидуальный набор требований безопасности, который в наибольшей степени учитывает их особенности, среду функционирования и угрозы безопасности, существующие в данной среде [9]. Этот подход является наиболее трудоемким и требует высокой квалификации эксперта. На качество результатов аудита в этом случае значительно влияет используемая методология анализа и управления рисками.

Рекомендуется обратить внимание на комплексный тип аудита, который может включать в себя, наряду с экспертным аудитом, элементы таких видов, как оценка соответствия и тестирование.

Анализируя применимость аудита пассивного и активного типов, отметим, что оба подвида могут быть использованы на практике в зависимости от целей и задач конкретной проверки. Обсуждая легальность мероприятий аудита, выбор однозначно делается в пользу легального подвида на основании принципа законности в сфере ИБ. Кроме этого, аудит ИБ вуза может сочетать в себе организационно-нормативные и технические формы, что повышает его результативность.

4. Рекомендуемые подходы к проведению аудита и методы анализа данных. Среди подходов, используемых в процессе аудита, обычно выделяют два вида: практические подходы к проведению аудита и теоретические подходы, лежащие в его основании [11].

Наиболее адекватным практическим подходом для его реализации в учебных заведениях высшего уровня представляется комбинация анализа рисков и стандартов ИБ. Нормативные документы задают планку минимальному комплекту предписаний безопасности, предъявляемых к изучаемым объектам. Специфические нюансы конкретного вуза учитываются детальной оценкой рисков для его активов. Такой подход устраняет «минусы» аудита чисто на основе анализа рисков или только на соответствие стандартам. Поэтому целесообразно применять экспериментальное изучение системы безопасности объектов аудита вуза для ее реальной проверки и выявления ее «узких» мест и «слабых» звеньев.

Проанализировав варианты теоретических подходов, можно выделить их тип, базирующийся на моделях оценки, определяемых видом формализации процесса. В соответствии с этим подходом характеристики, описывающие состояние системы ИБ объектов, сравниваются с неким эталоном, чтобы их оценить и проверить, соответствуют ли они заложенным требованиям. Поскольку аудит информационной безопасности в вузах только «набирает обороты», подобный подход вполне адекватен. Для вуза целесообразен подход на основе «серого ящика», если выбирать его тип, определяемый доступностью информации о системе для специалиста аудита. Этот вид наилучшим образом учитывает специфику организации, возможное наличие конфиденциальной информации и предпочтительный внутренний подвид аудита.

Из изложенного следует, что в качестве методов анализа данных в процессе аудита следует рекомендовать к использованию анализ рисков и соответствие нормам ИБ.

5. Этапность проведения аудита. Последовательность проведения аудита является важным элементом организации проверки и служит основой для усиления безопасности деятельности вуза. Поэтапное проведение аудита создает возможности для более полного и объективного изучения текущего состояния и планов развития информационных технологий в конкретном вузе, сравнения результатов использования информационных технологий с альтернативными, разработки рекомендаций по усилению безопасности в сфере применения информационных технологий, а также оформления и представления результатов аудита. Именно такой подход может быть полезным для практики проведения аудиторской проверки в сфере образования.

Большинство авторов научных публикаций склонны к тому, что процесс аудита должен осуществляться в три этапа.

На начальном шаге идентифицируются объекты аудита, подбираются критерии и методология аудита, а также его средства и способы. На этом же этапе комплектуется коллектив аудиторов, оцениваются объем и масштаб аудита, фиксируются его сроки. На следующем шаге изучается состояние защищенности объектов, аккумулируется информация исследования угроз и уязвимостей объектов, анализируются полученные результаты и верстается промежуточный отчет. На третьем шаге формируется основной отчетный документ, включающий в себя описание набора мероприятий для повышения уровня безопасности имеющейся системы защиты активов объектов, а также план устранения «слабых» звеньев и недочетов в реализации ИБ.

Этапность проведения аудита целесообразно дополнить этапом сопровождения. Его потребность продиктована необходимостью периодического консультирования управленческого аппарата учебного заведения по внедрению в практику рекомендаций экспертов, внесению необходимых корректировок в их рекомендации. Тогда процесс аудита будет выглядеть следующим образом (*рис. 2*).

6. Организационно-технические основы аудита в вузе. Аудиторская проверка ИБ вуза должна основываться на базовом документе (пакете документов) организации, регламентирующем такого рода деятельность. Подобная норма обрисовывает основные цели и задачи, области, виды и направления, а также допустимые критерии оценки. Кроме этого, документ фиксирует порядок формирования состава коллектива аудиторов для внутреннего аудита и назначения руководителя этого коллектива. Форма типового договора (контракта) на проведение аудиторской проверки с ними также должна входить в состав базового пакета. Аспекты подобного договора разобраны в [7, с. 108].

Порядок организованного проведения аудита отражается в плане-графике проверки, которым руководствуются в ходе непосредственной реализации процесса. В состав базового пакета также входит и план систематических повторных проверок.

Исследования объектов аудита, если они предусмотрены планом проверки, проводятся на основании программы и методики испытаний, которые должны быть своевременно подготовлены и утверждены. Результаты практических опытных

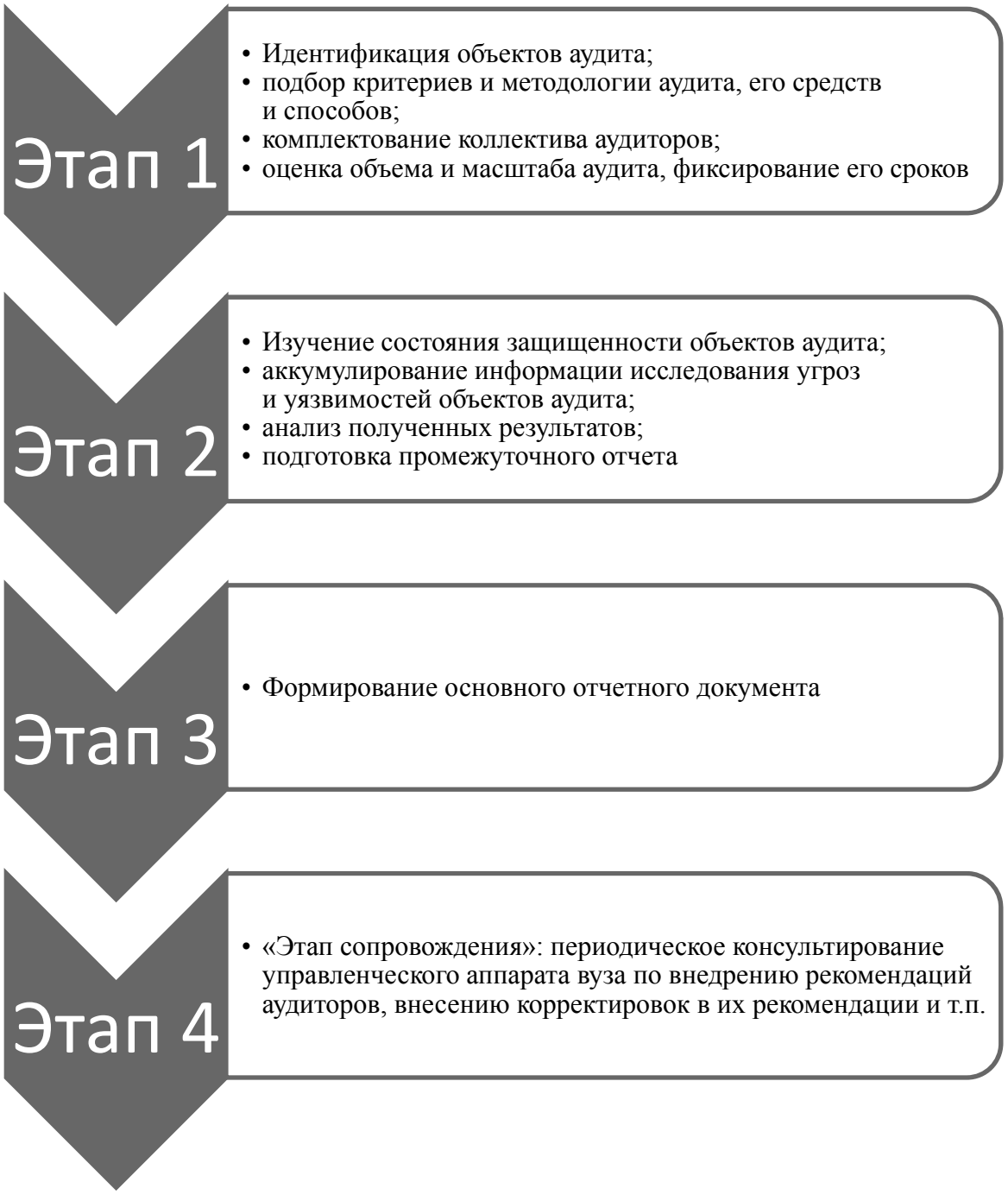

Рис. 2 / Fig. 2. **Основные этапы проведения аудита информационной безопасности вуза / The main stages of the information security auditing at a university**

Источник / Source: разработано авторами / developed by the authors.

проверок заносятся в протоколы или оформляются в виде техотчетов, являющихся частью пакета итоговых документов.

Аудит информационной безопасности высшей школы следует понимать не только как инвентаризацию используемых аппаратно-программных средств для обнаружения «пиратских» версий, но и как возможность оценки работы пользователей вуза и сотрудников служб безопасности, их трудовой дисциплины и способности внедрять и эксплуатировать новые информационные технологии.

Проблемы ИБ в организациях высшего образования касаются всех сотрудников, преподавателей и студентов. Необходимо дополнить учебные планы

вузов дисциплиной «Информационная безопасность» для подготовки бакалавров, специалистов и магистров, а также регулярно проводить повышение квалификации профессорско-преподавательского состава высшей школы в этом направлении. Такой опыт накоплен в ННГУ им. Н.И. Лобачевского при подготовке экономистов, финансистов и менеджеров.

7. Состав результатов аудита вуза. Содержание этой составляющей формируется решениями поставленных задач аудита. Результаты обобщаются в пакете итоговых документов, который должен содержать:

- оценку объектов аудита на соответствие требованиям к уровню их информационной безопасности;
- описание состояния актуальной защищенности объектов;
- ранжированный список рисков, обусловленных возможным воплощением в реальность информационных угроз;
- соответствие изучаемых объектов и системы их защиты требованиям норм по ИБ и положениям документа о политике безопасности вуза;
- детализированные рекомендации по совершенствованию системы защиты информации, внедрению новых и повышению эффективности существующих механизмов безопасности ИС вуза.

Эти рекомендации необходимо реализовывать по следующим направлениям:

- разработка системы информационного обеспечения рабочих мест преподавателей, управленческого звена вуза;
- установление схем обмена информацией;
- создание системы контроля за работой программного обеспечения и его пользователями;
- систематический контроль за изменениями в программном обеспечении;
- осуществление мероприятий по сохранению конфиденциальности данных.

Необходимо, чтобы результирующий отчет содержал описание изменений, произошедших в системе с момента предыдущей аудиторской проверки, а также рекомендуемую дату последующего мероприятия.

ЗАКЛЮЧЕНИЕ

Проведение аудиторских проверок на базе рассмотренной концепции позволит усовершенствовать комплексную систему ИБ вуза и снизить уровень рисков, обусловленных возможной реализацией угроз ИБ. Уменьшение вероятности подобного рода инцидентов приведет к увеличению результативности использования современных информационных технологий в учреждении высшего образования, что, в свою очередь, повысит эффективность функционирования вуза в целом.

Включение в состав объектов аудита информационно-образовательных процессов позволит не только проанализировать и повысить уровень защиты конфиденциальной информации, циркулирующей в ИС организации, но и обеспечить оценку уровня доступа к сведениям, необходимым учащимся для подготовки к занятиям.

Проведение внутреннего аудита с использованием собственного квалифицированного персонала учреждения позволит снизить финансовые издержки на его реализацию при возможном минимальном снижении качества проводимых работ.

Рекомендуемая оценка изменений, произошедших в системе ИБ с момента предыдущей проверки, позволит донести до администрации вуза динамику уровня информационной безопасности организации, состояние объектов аудита и системы их защиты по сравнению с предыдущей проверкой и, соответственно, необходимость последующих мероприятий.

Применение положений предложенной концепции аудита ИБ на практике позволит проводить мониторинг исполнения федеральных законов и программ в образовательном заведении и согласовывать местные практики с нормативными документами вышестоящего уровня.

СПИСОК ИСТОЧНИКОВ

1. Завгородний В.И. Комплексная защита информации в компьютерных системах. М.: Логос; 2001. 264 с.
2. Беззубов А.Ф., Синицын И.В. Применение вычислительных систем отечественного производства как средство повышения информационной безопасности вуза. *Вестник Российской таможенной академии*. 2017;(2):106–110.
3. Козачок А.И., Левицкая Ю.А. Методы оценки информационных рисков в сетях учебного назначения. *Методические вопросы преподавания инфокоммуникаций в высшей школе.* 2012;1(4):27–29.
4. Стукалова О.В., Боякова Е.В., Юдушкина О.В. Системный подход к обеспечению информационной безопасности в образовательных организациях (на примере вузов). *Вестник НЦБЖД.* 2017;32(2):104–109.

5. Тюменев А.В., Панов Н.Н. Комплексная информационная безопасность в вузе. *Экстремальная деятельность человека.* 2018;47(1):65–68.
6. Шабанов А.А. Предпосылки формирования системы информационной безопасности в вузах. *Конкурентоспособность в глобальном мире: экономика, наука, технологии.* 2017;5–2(44):177–180.
7. Ситнов А.А. Организация аудита информационной безопасности. *Учет. Анализ. Аудит.* 2016;3(6):102–110.
8. Курило А.П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. М.: БДЦ-пресс; 2006. 304 с.
9. Козьминых С.И., Козьминых П.С. Аудит информационной безопасности. *Вестник Московского университета МВД России.* 2016;(1):181–186.
10. Горюнов А.Г. Внутренний аудит информационной безопасности предприятия. *Вестник Московского университета МВД России.* 2012;(8):227–231.
11. Макаренко С.И. Аудит информационной безопасности: основные этапы, концептуальные основы, классификация мероприятий. *Системы управления, связи и безопасности.* 2018;(1):1–29.
12. Mahfuth A., Bakar A.A., Yussof S., Ali N. A systematic literature review: Information security culture. In: 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). DOI: 10.1109/ICRIIS.2017.8002442

REFERENCES

1. Zavgorognii V.I. Comprehensive protection of information in computer systems. Moscow: Logos; 2001. 264 p. (In Russ.).
2. Bezzubov A.F., Sinitsyn I.V. The use of computer systems of domestic production as a means of improving a University information security. *Vestnik Rossiiskoi tamozhennoi akademii = The Russian Customs Academy Messenger.* 2017;(2):106–110. (In Russ.).
3. Kozachok A.I., Levitskaya Yu.A. Methods of assessing information risks in networks for educational purposes. *Metodicheskie voprosy prepodavaniya infokommunikatsyi v vyschei schkole = Methodical Questions of Teaching of Information and Communication in High School.* 2012;1(4):27–29. (In Russ.).
4. Stukalova O.V., Boyakova E.V., Yudushkina O.V. A systematic approach to ensuring information security in educational organizations (on the example of universities). *Vestnik NTsBZhD = Journal of the Scientific Center for Life Safety.* 2017;32(2):104–109. (In Russ.).
5. Tyumenev A.V., Panov N.N. Comprehensive information security at the university. *Ekstremal'naya deyatel'nost' cheloveka = Extreme Human Activity.* 2018;47(1):65–68. (In Russ.).
6. Shabanov A.A. Preconditions of formation of system of information security in universities. *Konkurentosposobnost' v global'nom mire: ekonomika, nauka, tekhnologii = Competitiveness in a Global World: Economics, Science, Technology.* 2017;5–2(44):177–180. (In Russ.).
7. Sitnov A.A. The Organization of Auditing of Information Security. *Uchet. Analiz. Audit = Accounting. Analysis. Auditing.* 2016;3(6):102–110. (In Russ.).
8. Kurilo A.P., Zefirov S.L., Golovanov V.B. et al. Audit of information security. Moscow: BDTs-press; 2006. 304 p. (In Russ.).
9. Koz'minykh S.I., Koz'minykh P.S. Information security auditing. *Vestnik Moskovskogo universiteta MVD Rossii = Bulletin of the Moscow University of the Ministry of Internal Affairs of the Russian Federation.* 2016;(1):181–186. (In Russ.).
10. Goryunov A.G. Internal auditing of the information security of the company. *Vestnik Moskovskogo universiteta MVD Rossii = Bulletin of the Moscow University of the Ministry of Internal Affairs of the Russian Federation.* 2012;(8):227–231. (In Russ.).
11. Makarenko S.I. Audit of information security: The main stages, conceptual framework, classification of types. *Sistemy upravleniya, svyazi i bezopasnosti = Systems of Control, Communication and Security.* 2018;(1):1–29. (In Russ.).
12. Mahfuth A., Bakar A.A., Yussof S., Ali N. A systematic literature review: Information security culture. In: 2017 International Conference on Research and Innovation in Information Systems (ICRIIS). DOI: 10.1109/ICRIIS.2017.8002442

ИНФОРМАЦИЯ ОБ АВТОРАХ

Вячеслав Николаевич Ясенев — кандидат экономических наук, профессор кафедры информационных технологий и инструментальных методов в экономике Института экономики и предпринимательства, Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, Россия
yasenev@fnf.unn.ru
Артем Владиславович Дорожкин — кандидат экономических наук, доцент кафедры информационных технологий и инструментальных методов в экономике Института экономики и предпринимательства, Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, Россия
dorozhkin_av@mail.ru
Андрей Львович Сочков — кандидат технических наук, доцент кафедры информационных технологий и инструментальных методов в экономике Института экономики и предпринимательства, Нижегородский государственный университет им. Н.И. Лобачевского, Нижний Новгород, Россия
an.so2009@yandex.ru

ABOUT THE AUTHORS

Vyacheslav N. Yasenev — Cand. Sci. (Econ.), Professor of the Department of Information Technology and Instrumental Methods of Economics of the Institute of Economics and Entrepreneurship, Lobachevsky State University of Nizhny Novgorod, Nizhny Novgorod, Russia
yasenev@fnf.unn.ru
Artem V. Dorozhkin — Cand. Sci. (Econ.), Associate Professor of the Department of Information Technology and Instrumental Methods of Economics of the Institute of Economics and Entrepreneurship, Lobachevsky State University of Nizhny Novgorod, Nizhny Novgorod, Russia
dorozhkin_av@mail.ru
Andrei L. Sochkov — Cand. Sci. (Tech.), Associate Professor of the Department of Information Technology and Instrumental Methods of Economics of the Institute of Economics and Entrepreneurship, Lobachevsky State University of Nizhny Novgorod, Nizhny Novgorod, Russia
an.so2009@yandex.ru

Заявленный вклад авторов:
Ясенев В.Н.— формулировка гипотезы исследования, подготовка обзора литературы, подготовка текста статьи.
Дорожкин А.В.— подготовка обзора литературы по теме исследования, подготовка текста статьи.
Сочков А.Л.— описание результатов анализа данных, подготовка текста статьи.

The declared contribution of the authors:
Yasenev V.N.— formulation of the research hypothesis, preparation of a literature review on the research topic, a description of the results, preparation of the text of the article.
Dorozhkin A.V.— preparation of literature review on the research topic, preparation of the text of the article.
Sochkov A.L.— description of the data analysis results, preparation of the text of the article.

Статья поступила в редакцию 15.07.2019; после рецензирования 21.08.2019; принята к публикации 13.09.2019.
Авторы прочитали и одобрили окончательный вариант рукописи.
The article was submitted on 15.07.2019; revised on 21.08.2019 and accepted for publication on 13.09.2019.
The authors read and approved the final version of the manuscript.