Интернет-журнал «Отходы и ресурсы» https://resources.today
Russian Journal of Resources, Conservation and Recycling

2023, Том 10, № 1 / 2023, Vol. 10, Iss. 1 https://resources.today/issue-1-2023.html

URL статьи: https://resources.today/PDF/62ECOR123.pdf

DOI: 10.15862/62ECOR123 (https://doi.org/10.15862/62ECOR123)

Ссылка для цитирования этой статьи:
Гукетлов, М. М. Ключевые особенности защиты конфиденциальной информации и их экономические последствия в аудиторской организации / М. М. Гукетлов // Отходы и ресурсы. — 2023. — Т. 10. — № 1. — URL: https://resources.today/PDF/62ECOR123.pdf DOI: 10.15862/62ECOR123

For citation:
Guketlov M.M. Key features of the protection of confidential information and their economic consequences in the audit organization. *Russian Journal of Resources, Conservation and Recycling*. 2023; 10(1): 62ECOR123. Available at: https://resources.today/PDF/62ECOR123.pdf. (In Russ., abstract in Eng.) DOI: 10.15862/62ECOR123

УДК 338

Гукетлов Мурат Мухамедович
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Факультет «Международных экономических отношений»
E-mail: mguketlov@bk.ru

Научный руководитель: **Прасолов Валерий Иванович**
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Доцент Департамента экономической безопасности и управления рисками
Кандидат политических наук
E-mail: VIPrasolov@fa.ru

Ключевые особенности защиты конфиденциальной информации и их экономические последствия в аудиторской организации

Аннотация. Автором научной публикации рассматривается проблематика защиты конфиденциальной информации в аудиторской организации на современном этапе развития рыночных отношений. По мнению автора, аудиторские организации должны уделять должное внимание защите конфиденциальной информации с целью минимизации потенциальных убытков. Были проанализированы современные виды информации по категориям доступа, угрозы конфиденциальной информации. Рассмотрена организация работы по защите конфиденциальной информации на примере деятельности компании ООО «Мосаудит». Вместе с тем уделено внимание изучению методологии и способов защиты конфиденциальной информации на практическом примере. В рамках указанной аудиторской организации проанализированы имеющиеся правовые механизмы защиты, которые закрепляются в локальных нормативных актах компании, а также организационные методы, которые включают себя применяемые компанией управленческие методы и решения, а также современные технические меры. Автором в данном направлении был избран комплексный подход по изучению всех сущностных аспектов объекта исследования, где также особое внимание было уделено составлению рекомендательных мер для аудиторской организации ООО «Мосаудит» на основании изученной документации и деятельности компании. Предложены актуальные варианты действий, которые могут быть применимы на практике, направленные на усиление защиты конфиденциальной информации в рамках компании, в том числе проанализирована эффективность предпринятых компанией мер. Были сделаны выводы относительно необходимости применять современные меры по защите информации, которые включают себя

не только инженерно-технические мероприятия, но и эффективный подход в сфере управления компании с применением имеющихся локальных нормативных актов. Кроме того, отмечается возможный негативный экономический эффект от низкого уровня информационной безопасности.

Ключевые слова: конфиденциальная информация; аудиторская организация; экономика организации; управление организацией; информационная безопасность; экономический эффект; защита конфиденциальной информации

Введение

В современных экономических условиях добиться успеха в предпринимательской деятельности, высокой прибыли, сохранения и развития бизнеса возможно при обеспечении экономической безопасности хозяйствующего субъекта. Одной из главнейших составляющих экономической безопасности организации является информационная безопасность. Вместе с развитием технологий повышается не только уровень защиты информации, но параллельно развиваются и технологии по неправомерному извлечению информации, в том числе конфиденциальной. Поскольку несанкционированное раскрытие конфиденциальной информации влечет за собой существенные экономические и репутационное убытки для организации, то следует особое внимание уделять аспектам защиты конфиденциальной информации.

Актуальность темы исследования обусловлена повышенной необходимостью хозяйственных субъектов обеспечивать информационную безопасность в современных экономических реалиях, одной составляющей которой и является защита конфиденциальной информации. Особенно это связано с деятельность аудиторских организаций, когда за раскрытие информации хозяйственный субъект несет еще большие риски. Возможности заполучить доступ к этой информации растут вместе с возможностями предотвратить неправомерный доступ к конфиденциальной информации.

Цель исследования заключается в анализе ключевых аспектов защиты конфиденциальной информации аудиторской организации и составлении рекомендаций для улучшения данной составляющей информационной безопасности.

Объектом исследования является информационная безопасность аудиторской организации.

Предметом исследования является механизм защиты конфиденциальной информации в аудиторской организации и пути его совершенствования.

1. Методы и материалы

При написании данной работы автором использовались следующие методы: сравнительный, статистический анализы, анализ и обобщение нормативно-правовых актов, научных исследований, табличные и графические способы визуализации данных.

Для достижения данной цели в работе были поставлены следующие задачи:

- изучить теоретические аспекты защиты конфиденциальной информации в аудиторском бизнесе;
- проанализировать существующие методы и способы защиты конфиденциальной информации в аудиторской организации;

- сформировать предложения и рекомендации по совершенствованию механизма защиты конфиденциальной информации, оценить их эффективность.

Исследование основывается на отечественных научных исследованиях, нормативно-правовых актов федерального и локального уровней, а также на исследовании внутренней документации аудиторской организации.

Исследование вопросов информационной и экономической безопасности хозяйственного субъекта основательно исследованы в трудах таких авторов, как: Авдийский В.И. [1], Миронова О.А. [2], Зиновьева Ю.С. [3], Власенко М.Н. [4], Шевко Н.Р. [5], Примакин А.И. [6], Голованова Н.Б. [7].

2. Результаты и обсуждения

Информация в условиях развития постиндустриального общества приобретает характер нового фактора производства, на котором основана работа огромного числа хозяйственных субъектов. Более того, по сути, информация становиться предметом их деятельности, объектом купли-продажи.

В связи с чем вопросы, связанные с защитой информации, становятся в один ряд по своей важности с вопросами по защите имущества, особенно если раскрытие этой информации ведет к существенным издержкам для организации.

Для аудиторских организаций аспекты информационной безопасности стоят особо остро ввиду имеющегося государственного регулирования. Так, например, в ФЗ от 30.12.2018 № 307 «Об аудиторской деятельности» закреплено понятие аудиторской тайны — «ее составляют любые сведения и документы, полученные и (или) составленные аудиторской организацией и ее работниками по результатам контрольных мероприятий»[1].

За несанкционированное разглашение аудиторской тайны аудиторская организация несет существенные имущественные риски, особенно это касается конфиденциальной информации. Она представляет собой любую информацию, после доступа которой лицо обязано не раскрывать ее третьим лицам без согласия ее обладателя. К ней также может относиться особенно важные категории информации, как содержащие государственную или коммерческую тайну[2].

Специфика аудиторского бизнеса позволяет определить ключевые виды информации характерные именно для этого рода деятельности. В аудиторской фирме основной объем информации, подлежащей защите, составляет конфиденциальная информация, связанная с профессиональной деятельностью, что и составляет собой аудиторскую тайну. Кроме того, подлежат защите персональные данные сотрудников, документы, в которых содержится коммерческая тайна. Поскольку исследованная аудиторская фирма ООО «Мосаудит» осуществляет, в числе прочих, контрольные мероприятия в организациях оборонно-промышленного комплекса, существует комплекс обязательных мероприятий, направленных на защиту информации, составляющей государственную тайну.

[1] Федеральный закон от 30.12.2008 № 307-ФЗ "Об аудиторской деятельности" (с изм. от 31 декабря 2017 г.) // Собрание законодательства Российской Федерации. №1. 2009.

[2] Указ Президента Российской Федерации от 06.03.1997 № 188 «Об утверждении перечня сведений конфиденциального характера» // Собрание законодательства Российской Федерации. № 10. 1997.

Работа с конфиденциальной информацией предполагает определение основных источников, на основе которых выстраивается система защиты конфиденциальной информации. К основным источникам конфиденциальной информации в аудиторской организации можно отнести персонал фирмы, документы, технические средства (серверы, компьютеры, диски, флеш-карты и другие), коммуникационные средства, которые используются для передачи информации (телефоны, факсы и т. д.), передаваемые по каналам связи сообщения, содержащие конфиденциальную информацию.

В связи с существенным объемом поступающей информации в аудиторскую организацию возникает целый ряд угроз конфиденциальной информации. Это представляет собой возможные действия по раскрытию информации третьим лицам без санкции обладателя, причем это может происходить как изнутри (раскрытие информации одним из работников организации), так извне (взлом технической аппаратуры организации с целью получения дальнейшего доступа к информации).

Основные типы угроз конфиденциальной информации представлены на рисунке.

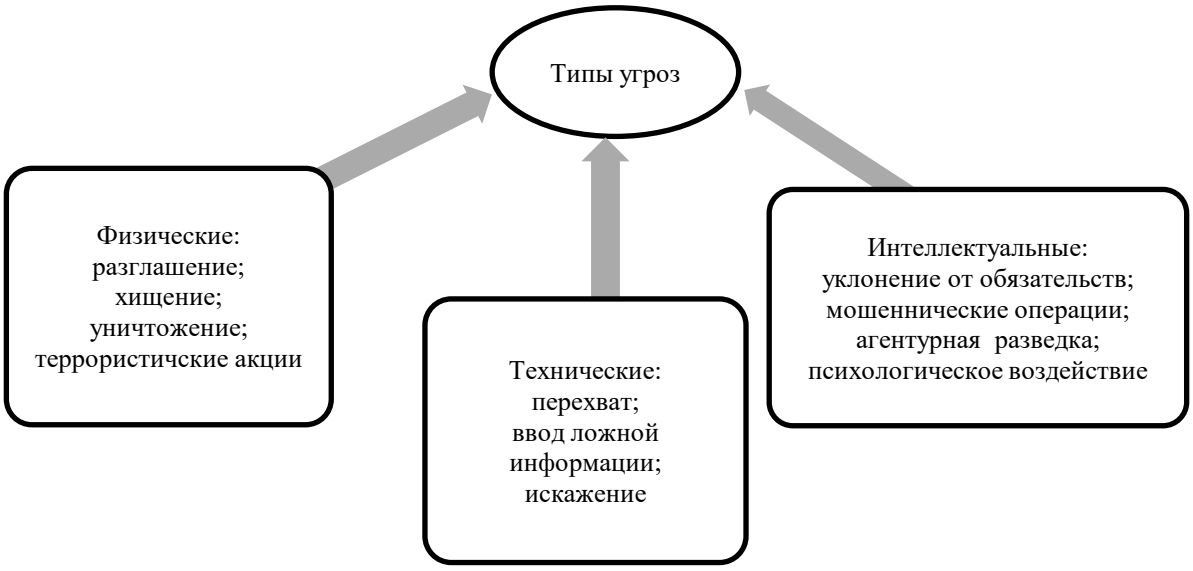

Рисунок 1. *Угрозы конфиденциальной информации [7]*

Перечисленные выше недобросовестные методы овладения конфиденциальной информацией на протяжении многих лет препятствуют бесперебойному функционированию аудиторских фирм. Присутствие на рынке значительного количества компаний порождает высокую конкуренцию и повышает вероятность применения нечестных методов конкурентной борьбы. Чтобы противостоять этому и оставаться на плаву, менеджменту компании необходимо грамотно организовать комплексную систему защиты конфиденциальной информации.

Деятельность по защите получаемой и хранящейся информации имеет ключевое значение для аудиторских фирм. В связи с этим возникает потребность в решении комплекса задач для поддержания безопасности информационных ресурсов компании. С целью недопущения раскрытия конфиденциальной информации аудиторские организации прибегают к полноценному созданию системы по защите информации через нормативно-правовую документацию и создание соответствующей технической инфраструктуры, которая бы затрагивала деятельность каждого работника организации и также взаимодействие с контрагентами.

Работа по защите информации от такого широкого круга угроз будет эффективна только в том случае, если существует четкое представление о требуемом уровне контроля за тем или иным источником конфиденциальной информации. В связи с этим, немаловажным элементом при формировании системы защиты конфиденциальной информации является определение необходимого уровня безопасности информационных ресурсов в процессе аналитических исследований. По их результатам формируют структуру и производят расчет эффективности системы защиты информационных ресурсов с учетом финансовых возможностей фирмы.

К практическим методам защиты конфиденциальной информации относят: юридические (разработка локальных актов, должностных инструкций, регламентирующих работу с конфиденциальной информацией, разработка положений в трудовых и гражданско-правовых договорах, предусматривающих обязательства о неразглашении конфиденциальной информации и ответственность за их несоблюдение, защита в суде и др.); организационные (ограничение доступа к конфиденциальной информации, обеспечение сохранности носителей информации, обучение работников по вопросам защиты тайны, ведение дел и журналов, их регистрация и учет, контроль порядка уничтожения документов и другие); физические (охрана помещений, пропускной режим); технические, программные, криптографические. Как правило, действенное функционирование системы защиты конфиденциальной информации достигается за счет комплексного применения указанных методов.

Рассмотрим далее предмет исследования относительно деятельности аудиторской организации ООО «Мосаудит». В целях предотвращения рисков, связанных с финансовыми, репутационными потерями, в ООО «Мосаудит» функционирует отдел экономической безопасности и защиты информации, основными видами деятельности которого являются защита конфиденциальной и иной информации ограниченного доступа, сбор и обработка информации о юридических лицах — заказчиках услуг, конкурентах (например, анализ учредительных документов, электронных ресурсов и т. д.), организация контроля доступа в офис организации и другие.

Существует три основных метода исследования механизмов защиты информации: анализ рисков, оценка соответствия стандартам и законодательным актам, комбинированный метод. Недостаток первых двух заключается в их неполном охвате существующей проблематики, который в достаточной степени компенсируется применением комбинированного метода.

Основополагающей частью механизма защиты информации фирмы является процесс выявления и регламентации реального перечня ценной информации, составляющей тайну хозяйствующего субъекта [8]. В соответствии с локально-нормативными актами ООО «Мосаудит», к таковой отнесены: сведения, составляющие государственную тайну, профессиональная тайна, персональные данные, коммерческая тайна. Все они разделены по уровню конфиденциальности: «секретно», «строго конфиденциально», «конфиденциально».

В целях разработки мероприятий по предотвращению потенциальных угроз информационной безопасности компании сотрудниками отдела экономической безопасности и защиты информации разработана матрица событий, угроз и обеспечения безопасности в отношении информационной безопасности ООО «Мосаудит». Анализируя изложенное, можно сделать вывод, что основные угрозы информационной безопасности могут исходить непосредственно от персонала организации, конкурентов.

В целях предотвращения угроз в ООО «Мосаудит» разработан механизм защиты информации, включающий несколько элементов, одним из которых является правовой. В том числе приказом генерального директора организации утверждена инструкция, детализирующая

процедуры доступа к конфиденциальной информации, должностные инструкции, содержащие положения о работе с данной информацией и обязательства по ее защите.

При приеме на работу каждый сотрудник подписывает трудовой договор и обязательство, содержащие положения об обязанности работника не разглашать конфиденциальные сведения фирмы и мерах ответственности за их разглашение, несанкционированное уничтожение или фальсификацию. Каждому сотруднику устанавливается 3-месячный испытательный срок. Кроме того, в ООО «Мосаудит» применяется Руководство по корпоративному поведению, профессиональные стандарты аудиторской деятельности и другие нормативные акты для решения проблем безопасности.

При решении проблем информационной безопасности ООО «Мосаудит» взаимодействует с различными государственными органами, в том числе: УВД по ЦАО ГУ МВД по г. Москве, Прокуратура ЦАО города Москвы, УФСБ по Москве и Московской области, Главное Управление МЧС по г. Москве, и др. Кроме того, осуществляется взаимодействие со службами экономической безопасности других хозяйствующих субъектов, клиентами фирмы. Заключен договор с Частным охранным предприятием ООО «Охрана» на оказание последним услуг по охране офисного здания ООО «Мосаудит» и прилегающей территории; с УВД по ЦАО г. Москвы (кнопка тревожной сигнализации).

Таким образом, можно сделать вывод о том, что механизм защиты конфиденциальной информации, реализуемый в ООО «Мосаудит», в определенной степени позволяет выполнять поставленные задачи по ведению бизнеса [9].

Между тем, принимая во внимание быстро меняющийся рынок технических средств защиты информации и устройств, позволяющих ее добывать, можно сделать вывод о необходимости усовершенствования технической составляющей системы защиты информации в ООО «Мосаудит» путем использования сертифицированных средств защиты, входящих в Государственный реестр сертифицированных средств защиты информации ФСТЭК N РОСС RU.0001.01БИ00.

Использование системы электронного документооборота в деятельности организации повышает результативность обработки и хранения информации, но в то же время порождает и новые риски, где отсутствие должного внимания к средствам защиты может привести к новым угрозам конфиденциальности. Перечень наиболее распространенных угроз для имеющейся системы электронного документооборота представлены ниже.

Таблица 1

Наиболее распространенные угрозы для системы документооборота

№п/п	Тип угроз	Характерные черты
1	2	3
1	Угроза целостности информационной системы	Повреждение, уничтожение, искажение информации как преднамеренного, так и непреднамеренного характера
2	Угроза конфиденциальности информационной системы	Кража, перехват, изменения маршрутов следования информации
3	Угроза работоспособности информационной системы	Умышленные атаки, ошибки администраторов и пользователей, сбои в оборудовании и программном обеспечении

Составлено автором

Учитывая, что персонал является важным субъектом в области информационной безопасности аудиторской деятельности, представляются недостаточными организационные меры по работе с кадровым составом. Требуются дополнительные правовые меры, регулирующие взаимоотношения с юридическими лицами в целях защиты конфиденциальной информации. В целях реализации такого принципа информационной безопасности как

своевременность, т. е. упреждающего характера мер по ее обеспечению, необходимо периодическое проведение аудита информационной безопасности организации [10].

На основе существующего механизма защиты конфиденциальной информации в указанной аудиторской организации автор составил следующие рекомендации по принятию дополнительных мер по обеспечению должного уровня защиты конфиденциальной информации.

В качестве дополнительных организационных мер по работе с кадровым составом целесообразно проводить периодическое повышение квалификации сотрудников отдела экономической безопасности и защиты информации. Например, обучение по программе профессиональной подготовки Информационная безопасность», согласованной со ФСТЭК, ФСБ России и Учебно-методическим объединением по образованию в области информационной безопасности, 26 направленной на формирование профессиональных компетенций, необходимых для профессиональной деятельности в области обеспечения информационной безопасности и комплексной защиты объектов информатизации [11].

Важное значение имеет совершенствование системы мотиваций персонала с целью повышения служебной дисциплины. В том числе применение сдерживающих средств мотивации, таких как лишение премиальных выплат, вынесение замечания, выговора по результатам установленных фактов несоблюдения требований в сфере защиты конфиденциальной информации, потенциально способствующих ее разглашению (утрате, искажению). С юридическими лицами, с которыми предполагается обмен сведениями, содержащими конфиденциальную информацию, представляется целесообразным заключать NDA (non-disclosure agreement) — соглашение о неразглашении, согласованное юридическими подразделениями обеих организаций [12].

Внешний аудит информационной безопасности целесообразно проводить раз в три года силами организации, представляющей консалтинговые услуги в данной области. Основной целью внешнего аудита является независимый анализ информационной защиты компании с целью определение уровня достаточности, обоснованности и правомерности всех принимаемых решений в области информационной безопасности.

Низкий уровень информационной безопасности хозяйствующего субъекта может привести к серьезным экономическим последствиям, таким как несанкционированный доступ к конфиденциальной информации, ее утечка или уничтожение. В таких случаях компания может столкнуться с негативными последствиями в виде убытков, снижения прибыли, судебных исков и ущерба репутации.

Например, если данные клиентов становятся доступными для третьих лиц, это может привести к утечке финансовой и личной информации, что может стать причиной судебных исков и потери доверия со стороны клиентов. Кроме того, нарушение информационной безопасности может привести к снижению объемов продаж и прибыли, так как клиенты и партнеры могут уходить к конкурентам, которые обеспечивают более высокий уровень безопасности.

Для минимизации рисков нарушения информационной безопасности важно принимать меры по ее улучшению. Например, компания может установить мощные системы защиты, регулярно проводить аудит информационных систем, обучать сотрудников правилам безопасности и контролировать доступ к конфиденциальной информации. Эти меры помогут не только улучшить безопасность, но и повысить доверие со стороны клиентов и партнеров, что, в свою очередь, позитивно скажется на репутации и прибыли компании.

Выводы

Система защиты информации представляет собой строго регламентированный процесс, направленный на предупреждение и выявление действий, нарушающих целостность, достоверность и конфиденциальность информационных ресурсов. Для аудиторской организации создание надежных механизмов защиты конфиденциальной информации имеет особенное значение, поскольку законодательно закреплена ее обязанность соблюдать требование об обеспечении конфиденциальности информации, составляющей аудиторскую тайну. Изучаемый хозяйствующий субъект располагает также конфиденциальной информацией, содержащей персональные данные сотрудников, коммерческую тайну. В результате исследования установлено, что действующий механизм защиты конфиденциальной информации имеет ряд недостатков в его технической, организационной и правовой составляющей. Утрата конфиденциальной информации может повлечь для ООО «Мосаудит» значительные репутационные потери, финансовые потери, вызванные дисциплинарными мерами ответственности, налагаемыми регуляторами, и мерами гражданско-правового характера, вплоть до потери бизнеса.

По результатам исследования предложены экономически целесообразные меры по совершенствованию механизма защиты конфиденциальной информации, с учетом которых хозяйствующий субъект может отвечать современным требованиям, обеспечивающим должный уровень защиты информации, что способствует дальнейшему экономическому развитию фирмы. Действенность механизма достигается за счет комплексного применения соответствующего режима охраны учреждения, организации конфиденциального делопроизводства, мероприятий по работе с кадрами, применения современных сертифицированных технических средств безопасности и защиты информации, эффективной информационно-аналитической деятельности, а также совокупности правовых, иных организационных и инженерно-технических мероприятий. При этом выстроенная система защиты должна периодически совершенствоваться с учетом потенциальных угроз, исходящих от технических новаций и иных источников.

ЛИТЕРАТУРА

1. Авдийский В.И. Роль стандартов экономической безопасности в системе мер обеспечения экономической безопасности хозяйствующих субъектов // Экономическая безопасность России: проблемы и перспективы. — 2014. — С. 294–313.
2. Миронова О.А. Экономическая безопасность: проблемы и пути ее обеспечения // Экономика. Налоги. Право. — 2015. — № 1. — С. 79–83.
3. Зиновьева Ю.С., Муругова М.С. Значение учетно-отчетной информации в обеспечении экономической безопасности хозяйствующих субъектов // Учет и статистика. — 2016. — № 4(44). — С. 10–20.
4. Власенко М.Н., Унижаев Н.В. Информационно-аналитическое обеспечение принятия управленческих решений-значимый фактор повышения экономической безопасности хозяйствующих субъектов в условиях развития рыночной системы хозяйствования // Национальные интересы: приоритеты и безопасность. — 2010. — № 33. — С. 59–69.
5. Шевко Н.Р. Информационная составляющая экономической безопасности: необходимость обеспечения защищенности // Ученые записки Казанского юридического института МВД России. — 2016. — Т. 1. — № 2(2). — С. 160–164.

6. Примакин А.И., Большакова Л.В. Модель оценки уровня экономической безопасности хозяйствующего субъекта // Вестник Санкт-Петербургского университета МВД России. — 2012. — Т. 56. — № 4. — С. 139–145.
7. Голованова Н.Б. Формирование подходов к оценке экономической безопасности субъекта хозяйствования // Доклады Томского государственного университета систем управления и радиоэлектроники. — 2014. — № 2(32). — С. 294–302.
8. Гашо И.А., Иовлева О.В., Токарь Е.В. К вопросу о сущности имущественной безопасности и ее роли в системе безопасности // Вестник Белгородского университета кооперации, экономики и права. — 2019. — № 2. — С. 95–106.
9. Токмакова Е.Г., Юхтанова Ю.А., Скипин Д.Л. Формирование информации о потерях хозяйствующего субъекта в бухгалтерском учете для обеспечения его экономической безопасности // Учет. Анализ. Аудит. — 2020. — Т. 7. — № 1. — С. 49–57.
10. Бердникова Л.Ф., Груздев Г.В. К вопросу о функциональных стратегиях системы экономической безопасности предприятия // Азимут научных исследований: экономика и управление. — 2017. — Т. 6. — № 4(21). — С. 54–56.
11. Маняева В.А. и др. Учетная политика для целей обеспечения экономической безопасности коммерческой организации // Вестник Самарского государственного экономического университета. — 2017. — № 8. — С. 76–84.
12. Шаповалова И.М. Теоретические подходы к определению понятия "экономическая безопасность субъектов хозяйствования" // Азимут научных исследований: экономика и управление. — 2019. — Т. 8. — № 1(26). — С. 397–400.

Guketlov Murat Mukhamedovich
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: mguketlov@bk.ru

Academic adviser: **Prasolov Valeriy Ivanovich**
Financial University under the Government of the Russian Federation, Moscow, Russia
E-mail: VIPrasolov@fa.ru

Key features of the protection of confidential information and their economic consequences in the audit organization

Abstract. The author of a scientific publication considers the problem of protecting confidential information in an audit organization at the present stage of development of market relations. According to the author, audit organizations should pay due attention to the protection of confidential information in order to minimize potential losses. Modern types of information were analyzed by categories of access, threats to confidential information. The organization of work on the protection of confidential information is considered on the example of the activities of the company Mosaudit LLC. At the same time, attention is paid to the study of the methodology and methods for protecting confidential information on a practical example. Within the framework of the specified audit organization, the existing legal protection mechanisms are analyzed, which are fixed in the company's local regulations, as well as organizational methods, which include the management methods and solutions used by the company, as well as modern technical measures. In this direction, the author chose an integrated approach to study all the essential aspects of the object of study, where special attention was also paid to the preparation of recommendatory measures for the audit organization Mosaudit LLC based on the studied documentation and the company's activities. Relevant options for action are proposed that can be applied in practice, aimed at strengthening the protection of confidential information within the company, including the analysis of the effectiveness of the measures taken by the company. Conclusions were drawn regarding the need to apply modern measures to protect information, which include not only engineering and technical measures, but also an effective approach in the field of company management using existing local regulations. In addition, there is a possible negative economic effect from a low level of information security.

Keywords: confidential information; audit organization; organization economics; organization management; information security; economic effect; protection of confidential information