www.volsu.ru

DOI: https://doi.org/10.15688/ek.jvolsu.2025.1.11

UDC 65.012.72
LBC 65.052.8

Submitted: 09.01.2025
Accepted: 25.01.2025

IT AUDIT: CONTROL OF ACCESS RIGHTS AND SEGREGATION OF DUTIES

Salavat D. Daudov
OOO Gazprom Dobycha Astrakhan, Astrakhan, Russian Federation

Adelia M. Duisalieva
OOO Gazprom Dobycha Astrakhan, Astrakhan, Russian Federation

Abstract. IT audit plays a major role in ensuring the safety and reliability of the use of an organization's information systems. It is responsible for assessing the effectiveness of the organization's internal control in the field of information security, identifying potential risks, and finding ways to minimize them. The article defines the main areas of conducting an IT audit and examines in more detail the audit of the distribution of access rights to IT systems, since granting users excessive access rights can lead to the implementation of the following risks: unavailability of the company's services and information systems, data compromise, fraudulent transactions, and unintentional errors. The article examines in more detail the principle of segregation of duties (SoD) as a mechanism for ensuring the reliability of the access management process and reducing the risks identified in this area. An algorithm of actions that must be taken to implement an SoD system in an organization is given, namely: analyze business processes, assess risks, separate processes and functions, distribute roles and responsibilities, implement access controls, and monitor processes and functions. As one of the practices for implementing a system of segregation of duties, the formation of an SoD matrix is proposed for both business processes in general (segregation of duties by positions) and for individual information systems (segregation of duties by roles).

Key words: IT audit, IT risks, access management, principle of segregation of duties, duties conflict, SoD matrix, information security.

Citation. Daudov S.D., Duisalieva A.M. IT Audit: Control of Access Rights and Segregation of Duties. *Vestnik Volgogradskogo gosudarstvennogo universiteta. Ekonomika* [Journal of Volgograd State University. Economics], 2025, vol. 27, no. 1, pp. 133-143. (in Russian). DOI: https://doi.org/10.15688/ek.jvolsu.2025.1.11

УДК 65.012.72
ББК 65.052.8

Дата поступления статьи: 09.01.2025
Дата принятия статьи: 25.01.2025

IT-АУДИТ: КОНТРОЛЬ ПРАВ ДОСТУПА И РАЗГРАНИЧЕНИЯ ПОЛНОМОЧИЙ

Салават Джигангирович Даудов
ООО «Газпром добыча Астрахань», г. Астрахань, Российская Федерация

Аделя Мадиевна Дуйсалиева
ООО «Газпром добыча Астрахань», г. Астрахань, Российская Федерация

Аннотация. IT-аудит играет большую роль в обеспечении безопасности и надежности использования информационных систем организации. Он отвечает за оценку эффективности внутреннего контроля организации в области информационной безопасности, выявление потенциальных рисков и путей для их минимизации. В статье определены основные направления проведения IT-аудита, более подробно рассмотрен аудит распределения прав доступа к информационным системам, поскольку наделение пользователей излишними правами доступа может привести к реализации следующих рисков: недоступность сервисов и информационных систем компании, компрометация данных, проведение мошеннических операций, совершение непреднамеренных ошибок. В статье более подробно рассмотрен принцип разделения полномочий (SoD) как механизм обеспечения надежности процесса управления доступом, снижения рисков, обозначенных

в этой области. Приведен алгоритм действий, которые необходимо предпринять в целях внедрения SoD-системы в организации, а именно: проанализировать бизнес-процессы, оценить риски, разделить процессы и функции, распределить роли и ответственность, внедрить контроли доступа, проводить мониторинг процессов и функций. В качестве одной из практик по внедрению системы разделения обязанностей предложено формирование SoD-матрицы как для бизнес-процессов в целом, так и для отдельных информационных систем.

Ключевые слова: IT-аудит, IT-риски, управление доступом, принцип разделения полномочий, конфликт полномочий, SoD-матрица, информационная безопасность.

Цитирование. Даудов С. Д., Дуйсалиева А. М. IT-аудит: контроль прав доступа и разграничения полномочий // Вестник Волгоградского государственного университета. Экономика. – 2025. – Т. 27, № 1. – С. 133–143. – DOI: https://doi.org/10.15688/ek.jvolsu.2025.1.11

Введение, актуальность темы

Резко возросшая роль информационных технологий в современной экономике, где ведущую роль играет работа с данными, без сомнения, является одной из наиболее важных тенденций в бизнесе последних десятилетий. В современных реалиях информация имеет все большее значение как для бизнеса, так и для государственных структур, поэтому происходит значительный рост хищений конфиденциальной информации и данных, которые приводят к возникновению морального ущерба, ухудшению деловой репутации, незаконному использованию интеллектуальной собственности. Согласно проведенным исследованиям, за первую половину 2023 г. в мире зафиксировано 5 532 случая утечки информации, что в 2,4 раза превышает показатель за тот же период 2022 г. (2 294 случая) [Черноусов].

Следует отметить, что мошеннические действия, связанные с хищением информации ограниченного доступа, наносящие как прямой действительный ущерб, так и вызывающие скрытые угрозы долговременного характера, совершаются не только конкурентами, но и работниками организации, которые действуют в целях дальнейшего вымогательства, шантажа, получения финансовой выгоды и т. д. Данные преступления, как правило, являются следствием отсутствия процедур защиты информации, действующих на постоянной основе в организации, а также нарушением разработанных регламентов. К таким событиям может приводить в том числе беспрепятственный доступ к документам случайных лиц или лиц, не имеющих на это полномочий [Каширская и др., 2022]. Именно поэтому тема обеспечения информационной безопасности хозяйствующих субъектов является достаточно актуальной и требует детального рассмотрения и уточнения методики аудита информационных систем, в том числе в части проверки процесса управления доступа к информационным системам. С учетом этой тенденции, главная задача внутреннего аудита – следовать за волной развития технологий и одновременно расширять свою роль в обеспечении сохранности и доступности информации, важной для бизнеса [Будущее кибербезопасности ...].

Научная новизна работы заключается в описании подходов к проведению аудиторских процедур контроля прав доступа и разграничения полномочий в рамках IT-аудита, а также в приведении алгоритма действий, которые необходимо предпринять в целях внедрения механизма разграничения полномочий пользователей в информационных системах.

Роль IT-аудита в обеспечении информационной безопасности

Внутренний аудит – деятельность по предоставлению независимых и объективных гарантий и консультаций, направленная на повышение стоимости и совершенствование работы компании. Внутренний аудит помогает компании достичь поставленных целей, используя систематизированный и последовательный подход к оценке и повышению эффективности процессов управления рисками, контроля и корпоративного управления.

В настоящее время активно развивается такое направление внутреннего аудита, как IT-аудит или аудит информационных систем, который представляет собой процесс сбора и анализа свидетельств для оценки того, насколько информационные системы и ее компоненты:

– адекватно обеспечивают сохранность активов;

– поддерживают целостность данных и систем;

– предоставляют соответствующую и надежную информацию;

– достигают целей компании;

– экономно используют ресурсы компании;

– имеют эффективные внутренние контроли, которые обеспечивают разумную уверенность в том, что цели достигнуты и нежелательные события будут предотвращены или замечены и исправлены своевременно.

Проведение IT-аудита имеет следующие цели:

– соблюдение правовых и нормативных требований;

– обеспечение конфиденциальности информации;

– обеспечение целостности информации;

– обеспечение надежности и доступности IT-сервисов и информационных систем;

– повышение эффективности IT [Нагаева и др.].

Задача IT-аудита в рамках регулярного аудита заключается в получении уверенности в том, что информационные системы, используемые для составления отчетности, работают надежно и корректно, поскольку разумная уверенность в надежности информационных систем, используемых для составления отчетности, позволяет существенно сократить объем выборки при проведении регулярного аудита.

Из вышеизложенного следует, что IT-аудит представляет собой изучение и экспертную оценку всей IT-инфраструктуры компании и отдельных ее частей. По результатам проведенной экспертизы заказчик, то есть руководство компании, узнает о текущем состоянии функционирования IT-инфраструктуры и IT-подразделения, а также о направлениях повышения их эффективности и оптимизации расходов компании. Следует отметить, что область исследования при проведении IT-аудита необязательно должна охватывать всю IT-среду компании. Предмет IT-аудита можно локализовать и оценивать часть IT-инфраструктуры [Кашин и др., 2022].

В научной литературе наиболее распространенная классификация типов IT-аудита в зависимости от объектов, процедур и объема проверок представлена следующим образом:

– аудит на соответствие установленным нормам и стандартам;

– аудит распределения прав доступа к IT-системам;

– аудит информационных процессов и оценка эффективности их внедрения;

– аудит IT-контроля, влияющего на формирование финансовой отчетности;

– аудит качественных характеристик информационных систем;

– функциональный аудит и аудит безопасности определенных IT-систем и сервисов [Сафонова и др., 2024].

Рассмотрим основные составляющие программы IT-аудита:

1. *Оценка эффективности информационных технологий:* правильный подход позволяет оценить эффективность информационных технологий в отдельных областях или во всей организации в целом и поможет составить надлежащий баланс между потребностями бизнеса и ресурсами, которыми располагает экономический субъект.

2. *Оценка инфраструктуры IT-подразделений:* проведение нагрузочных тестирований позволит оценить достаточность вычислительных мощностей текущим и будущим потребностям бизнеса.

3. *Оценка программного обеспечения (ПО):* позволит оценить соответствие имеющегося программного обеспечения потребностям бизнеса и выявленных уязвимостей (слабых мест) с точки зрения информационной безопасности.

4. *Оценка качества внедрения информационных систем и технологий:* дает возможность оценить внедрение информационных систем и определить их соответствие техническому заданию.

5. *Оценка эффективности внутреннего контроля:* согласно Закону Сарбейнза – Оксли (SOX, Федеральный закон, принятый в США в 2002 г., который направлен на противодействие мошенничеству в финансовой сфере и ужесточение контроля за финансовой отчетностью), Федеральному закону от 06.12.2011 № 402-ФЗ «О бухгалтерском учете», руководство организации должно разработать и поддерживать эффективную работу внутреннего

контроля. Оценка данного направления позволит выявить, насколько эффективно в компании выстроена система внутреннего контроля по направлению информационной безопасности, какие существуют слабые стороны, а также определить направления для совершенствования контрольных процедур [Кеворкова, 2021].

В ходе проведения IT-аудита целесообразно рассмотреть, каким образом решается вопрос мониторинга средств контроля обработки информации, которые функционируют с использованием информационных технологий. Это может включать в том числе следующее:

– *средства контроля для мониторинга сложной IT-среды*, которые предназначены для оценки непрерывной эффективности организации средств контроля обработки информации и их соответствующей модификации с учетом изменения условий или оценки операционной эффективности средств контроля обработки информации;

– *средства контроля, которые отвечают за мониторинг прав доступа*, применяемых в автоматизированных средствах контроля обработки информации и обеспечивающих разделение должностных обязанностей;

– *средства контроля, которые отвечают за мониторинг выявления и устранения ошибок или недостатков системы контроля*, связанных с автоматизацией подготовки финансовой отчетности.

Если рассматривать IT-систему со стороны рисков информационной безопасности, то все они могут повлиять на деятельность организации на всех уровнях контроля. IT-аудит выявляет и анализирует эти риски в целях разработки эффективных планов для текущей оценки системы контроля. Результатом проектов по IT-аудиту являются рекомендации по их осуществлению для устранения выявленных рисков [Кеворкова, 2021].

Аудит процесса управления доступом к информационным системам

В данной статье более подробно рассмотрим риски, связанные с наделением пользователей правами доступа, превышающими уровень, необходимый для выполнения порученных им обязанностей. Некорректная реализация процесса управления доступом увеличивает вероятность наступления следующих рисков:

– недоступность сервисов и информационных систем компании в результате эксплуатации учетных записей неавторизованных пользователей либо учетных записей пользователей с избыточными правами доступа;

– компрометация данных (утечка данных / внесение несанкционированных изменений в информационные системы компании) в результате эксплуатации учетных записей неавторизованных пользователей, либо учетных записей пользователей с избыточными правами доступа;

– проведение мошеннических операций, вызванных действиями работников в условиях наличия избыточных и/или конфликтующих прав доступа;

– непреднамеренные ошибки, которые не будут выявлены в ходе повседневной деятельности в результате совмещения нескольких критичных полномочий у одного сотрудника [Колодяжный, 2021].

Контроль за рисками доступа направлен на снижение возможности для сотрудника совершить ошибку или мошеннические действия и скрыть это в ходе повседневной деятельности. Внутренний аудит может проводить анализ доступа пользователей к ключевым данным и системам для проверки соответствия уровней доступа текущим ролям [Международные основы ...].

В рамках аудита доступа к информационным системам следует проверить:

– процесс управления доступом, в том числе выдачу новых прав доступа сотруднику, изменение или изъятие доступа, периодический пересмотр прав доступа, установление парольных политик, операционных систем и баз данных, контроль физического доступа для обеспечения безопасности и ограничения доступа к конкретным объектам или помещениям;

– наличие активных учетных записей уволенных сотрудников, учетные записи сотрудников внешней техподдержки, учетные записи неизвестного назначения, а также наличие владельца на каждую учетную запись;

– контроль избыточных прав доступа у пользователей компании, а также у технологических учетных записей (учетные записи с максимальными правами доступа или тестовые учетные записи с правами администратора).

Принцип разделения полномочий (SoD) как механизм управления доступом

Наивысшим уровнем обеспечения надежности процесса управления доступом является внедрение процедуры Segregation of Duties (SoD) или принципа разделения полномочий (обязанностей), который применяется для предотвращения возможных конфликтов интересов, превышения полномочий и совершения мошеннических действий, в некоторых случаях – ошибочных действий на техническом уровне.

Внедрение принципа разграничения полномочий (SoD) является составляющей частью системы внутреннего контроля и методологии управления рисками. На основании в том числе данного принципа строится и функционирует система управления рисками и внутреннего контроля организации. Принцип разделения обязанностей заключается в разграничении функций, исключающих совмещение одним лицом (структурным подразделением) функции авторизации, совершения, учета операций с определенными активами и контроля их исполнения. Перечень нормативных документов, определяющих необходимость разделения обязанностей между участниками бизнес-процессов, представлен в таблице 1.

Построение системы разделения полномочий – эффективная мера организации контроля бизнес-процессов. Система разделения полномочий, выстроенная с учетом особенностей и рисков, присущих сфере деятельности предприятия, обеспечивает:

– снижение рисков совершения пользователями преднамеренных и непреднамеренных ошибок и злоупотреблений;

– выявление случаев наделения пользователей конфликтными и излишними полномочиями как в бизнес-процессах, так и в IT-системах;

– снижение трудозатрат специалистов ИТ-подразделения, службы безопасности, внутреннего аудита и контролеров в области информационной безопасности в процессах предоставления доступа пользователям, анализе и аудите существующих прав доступа в IT-системах [Международные основы …].

Преднамеренное наделение пользователей излишними ролями создает уязвимости в системе управления рисками и внутреннего контроля, в том числе связанные с вероятной компрометацией данных, проведением мошеннических операций, совершением ошибок и т. д. Рассмотрим *примеры* ролей, сочетание которых формирует конфликты полномочий и возможность возникновения рисков (см. табл. 2).

Рассмотрим наиболее распространенные системные причины возникновения конфликтов полномочий при эксплуатации информационных систем:

1) недостаточное внимание к возможному возникновению конфликтов полномочий при внедрении системы управления предприятием и проектировании структуры ролей пользователей;

2) непродуманная структура ролей в системе, не позволяющая обеспечить надлежащее разграничение полномочий;

3) недостаточно продуманные процедуры срочного предоставления дополнительных

Таблица 1. **Нормативные документы в области SoD**

Table 1. **Regulatory documents in the field of SoD**

Российское законодательство	Международная практика
1. Федеральный закон от 06.12.2011 № 402-ФЗ «О бухгалтерском учете» (ст. 19)	1. Стандарты и доклады профессиональных организаций (ISACA COSO)
2. Российские государственные стандарты (семейство стандартов ГОСТ Р ИСО 31000, 27000, 27005, 27001)	2. МПСВА (Международные профессиональные стандарты внутреннего аудита), в том числе дополнительные руководства по аудиту применения ИТ (GTAG))
3. Письма Министерства финансов РФ, которые содержат рекомендации по организации и осуществлению внутреннего контроля (в том числе письмо № ПЗ-11/2013)	3. Зарубежные стандарты в области ИТ (например, COBIT)

Примечание. Составлено авторами по: [Нагаева и др.].

полномочий, которые не отзываются после того, как необходимость в них перестает существовать;

4) ограничения по количеству персонала в том или ином подразделении, препятствующие обеспечению корректного разделения полномочий;

5) изменение должностных обязанностей в результате приема новых сотрудников, увольнения сотрудников и перемещения сотрудников между подразделениями;

6) изменения в бизнес-процессах организации;

7) изменение организационной структуры компании;

8) избыточное количество пользователей с правами администратора;

9) отсутствие возможности мониторинга / доступности информации о конфликтах полномочий для нужд подразделений внутреннего контроля и внутреннего аудита.

Реализация концепции разделения обязанностей (SoD) в контексте кибербезопасности требует комплексного подхода, который включает оценку критических процессов и функций в организации, понимание рисков, связанных с нарушениями SoD, а также разработку и внедрение эффективных средств контроля SoD. Рассмотрим более детально пошаговые действия, которые необходимо выполнить при построении системы разделения обязанностей:

1. *Анализ бизнес-процессов.*

На данном этапе необходимо изучить имеющиеся бизнес-процессы, определить ключевые направления, которые существенно влияют на эффективность деятельности предприятия, а также те операции, при совершении которых возникает необходимость обеспечения безопасности конфиденциальности информации.

Для этого необходимо изучить документы, регламентирующие работу бизнес-процессов, провести интервью с владельцами процессов. Результатом проведенной работы станет сформированный перечень бизнес-процессов, подпроцессов и действий, выполняемых пользователями в информационных системах, а также за их пределами.

2. *Оценка рисков.*

После определения существенно важных процессов, влияющих на работу организации, в рамках внедрения концепции разделения обязанностей в первую очередь необходимо

Таблица 2. **Примеры конфликтов полномочий в информационных системах**

Table 2. **Examples of duties conflicts in information systems**

Пример 1				
Роль № 1		**Роль № 2**		**Риски при наделении пользователя конфликтующими ролями**
Наименование	**Функция**	**Наименование**	**Функция**	
«Исполнитель»	Внесение информации в систему, составление отчетных документов и т. д.	«Руководитель / Контролер»	Рассмотрение и утверждение результатов работы Исполнителя	Риск отсутствия контроля со стороны руководителя, применения исполнителем «формального» подхода к работе, проведения исполнителем без ведома руководителя операций мошеннического характера, приводящих к убыткам, потери репутации компании и т. д.
Пример 2				
Роль № 1		**Роль № 2**		**Риски при наделении пользователя конфликтующими ролями**
Наименование	**Функция**	**Наименование**	**Функция**	
«Специалист по социальным выплатам»	Внесение в систему информации о социальных выплатах	«Бухгалтер»	Начисление заработной платы и иных выплат	Риск отражения в системе несанкционированной социальной выплаты с последующим ее осуществлением, в том числе на расчетный счет стороннего лица (организации)
Пример 3				
Роль № 1		**Роль № 2**		**Риски при наделении пользователя конфликтующими ролями**
Наименование	**Функция**	**Наименование**	**Функция**	
«Сотрудник эксплуатационной службы (диспетчер автотранспорта)»	Организация и координация движения транспортных средств	«Сотрудник ремонтно-механической мастерской»	Проверка и подтверждение технического состояния транспортных средств	Риск выпуска на линию транспортных средств в состоянии, не предназначенном для эксплуатации, что может повлечь возникновение дорожно-транспортных происшествий

Примечание. Составлено авторами по результатам проведенных исследований.

провести работу по оценке рисков, включающую в себя:

– определение рисков, связанных с отсутствием разделения обязанностей между сотрудниками;

– определение уровня критичности этих рисков;

– согласование перечней рисков с владельцами бизнес-процессов, подпроцессов.

На этом этапе необходимо выявить и описать компенсирующие контрольные процедуры, а также идентифицировать дополнительные ограничения, относящиеся к доступу к критичным данным.

В результате проведенной работы будут сформированы:

– перечень рисков конфликтных полномочий, ранжированный по уровню критичности для бизнеса;

– перечень компенсирующих контролей в привязке к конфликтам полномочий;

– перечень дополнительных ограничений, относящихся к доступу к критичным данным.

3. *Разделение процессов и функций.*

На этом шаге необходимо разделить критические процессы и функции на более мелкие компоненты и назначить эти компоненты разным сотрудникам. Это гарантирует, что ни один человек не будет иметь полного контроля над процессом или функцией, снижая риск нарушений SoD [Суслова и др., 2023].

4. *Распределение ролей и ответственности.*

После разделения важнейших процессов и функций следующим шагом является распределение ролей и обязанностей между отдельными лицами. Этот этап включает в себя определение ответственности сотрудников за критически важными процессами и функциями, что является гарантом того, что отдельные лица могут выполнять только те задачи, на которые они уполномочены.

5. *Внедрение контроля доступа.*

Следующим шагом является внедрение контроля доступа для предотвращения несанкционированного доступа к критически важным системам и данным. На этом этапе происходит внедрение таких средств контроля, как брандмауэры (межсетевые экраны), системы обнаружения вторжений и шифрования для предотвращения несанкционированного доступа к конфиденциальной информации.

6. *Мониторинг процессов и функций.*

На данном этапе осуществляется мониторинг журналов доступа и системной активности для выявления потенциальных нарушений SoD, а также проведение регулярных аудитов критически важных систем и процессов, чтобы убедиться, что средства контроля SoD функционируют должным образом.

Одной из лучших практик по внедрению в компанию системы разделения обязанностей (SoD) в контексте кибербезопасности является создание SoD-матрицы, основная цель которой заключается в минимизации вероятности наступления рисков мошенничества, ошибок или действий, представляющих собой угрозу для компании.

SoD-матрица представляет собой двумерную таблицу, в которой отдельные сотрудники (роли) сопоставлены с различными задачами и полномочиями в рамках процесса. В SoD-матрице отражается распределение между сотрудниками обязанностей, таких как авторизация, аутентификация и доступ к данным и т. д., что позволяет сделать вывод о том, что один сотрудник (пользователь, наделенный определенными ролями) не может самостоятельно и бесконтрольно управлять критически важными процессами. Одной из наиболее важных предпосылок для создания SoD-матрицы является понимание того, что означает каждая обязанность и каковы лежащие в ее основе риски. В целях создания полезной для бизнеса SoD-матрицы необходимо определить, какие задачи легко выполнять одному и тому же сотруднику, а какие задачи необходимо разделить между сотрудниками для обеспечения информационной и экономической безопасности.

Разделив надлежащим образом различные задачи и функции, обозначив возможные риски, SoD-матрица позволяет проиллюстрировать масштабы проблем, связанных с возможными конфликтами соответствия требованиям, которые есть в каждом конкретном бизнес-процессе. Анализ существующей SoD-матрицы позволяет быстро определить, было ли четко выполнено требование соблюдения принципа разделения обязанностей по всем направлениям, или имеет место наде-

ление сотрудника или конкретной роли слишком большими полномочиями.

SoD-матрицы могут быть разработаны как для бизнес-процесса, или подпроцесса в целом, так и для отдельной информационной системы. При этом разделение полномочий может быть привязано к отдельным сотрудникам, исходя из обязанностей, установленных должностными инструкциями, или же к ролям информационной системы.

Рассмотрим *пример* разграничения функций в зависимости от занимаемой должности, то есть выполняемых обязанностей. В компании эксплуатируется информационная система «АВС», в которой функционируют 5 ролей: «Роль № 1» ... «Роль № 5». Основные пользователи системы – бухгалтер, закупщик, кладовщик и другие сотрудники. В компании предусмотрено распределение ролей между пользователями в соответствии с занимаемой должностью, то есть для каждой должности с учетом характера деятельности определен свой набор ролей, к которым сотрудники, занимающие эти должности, могут подключиться. С учетом разграничения полномочий, данное распределение может быть представлено следующим образом:

– Бухгалтер может подключиться только к Роли № 1 и № 2;

– Закупщик может подключиться только к Роли № 1 и № 3;

– Кладовщик может подключиться только к Роли № 1;

– Администратор информационной системы может подключиться только к Роли № 5; и т. д.

Таким образом, Бухгалтеру недоступны к подключению Роли № 3, 4, 5, а Кладовщик может подключиться только к одной Роли – № 3, остальные для него недоступны. Однако могут возникнуть ситуации, при которых необходимо срочное подключение пользователей, занимающих должности, не обозначенные в матрице разделения полномочий. В таком случае может возникнуть вопрос – какими ролями наделить пользователя таким образом, чтобы не предоставить излишний доступ к функционалу системы? Ответ на этот вопрос будет найден в SoD-матрице, составленной на основе определения несовместимости ролей информационной системы между собой.

На рисунке представлен пример оформления SoD-матрицы, отражающей конфликт полномочий в информационной системе «АВС» на основе разделения доступа по ролям. Как видно из рисунка, информационная система включает в себя 5 ролей, наделенных различным функционалом. При этом Роль № 5 не совместима с другими ролями, то есть если пользователь будет подключен к системе с этой ролью, то к другим ролям он подключиться не сможет, так как существует вероятность реализации определенного риска, обозначенного в примере «Риск С».

Роль № 1 совместима со всеми остальными ролями, за исключением Роли № 5, то-есть пользователь может одновременно подключить и Роль № 1, и Роль № 2, и т. д. в случае, если отсутствуют дополнительные ограничения, связанные с занимаемой должностью.

Роль № 2 и № 3 не совместимы из-за функциональных возможностей, которые конфликтуют между собой и не могут быть переданы одному пользователю в целях недопущения случаев возникновения «Риска А». Следовательно, пользователь не сможет подключиться к Роли № 2 и № 3 одновременно.

	Роль № 1	**Роль № 2**	**Роль № 3**	**Роль № 4**	**Роль № 5**
Роль № 1					*Риск С*
Роль № 2			*Риск А*		*Риск С*
Роль № 3		*Риск А*		*Риск В*	*Риск С*
Роль № 4			*Риск В*		*Риск С*
Роль № 5	*Риск С*	*Риск С*	*Риск С*	*Риск С*	

Рисунок. Пример SoD-матрицы для информационной системы «АВС»

Figure. Example of an SoD matrix for the information system “ABC”

Примечание. Составлено авторами по результатам проведенных исследований.

Из вышеизложенного следует, что грамотно составленная SoD-матрица станет хорошим помощником при подключении новых пользователей к системе, позволив избежать возникновения рисков, связанных с наделением пользователей излишними правами доступа.

Однако разработка и внедрение SoD-матрицы не гарантирует наличия постоянной защиты от рисков управления доступом. В целях соблюдения принципа разделения обязанностей, менеджменту следует рассмотреть возможность внедрения превентивных средств контроля, в том числе с использованием средств автоматизации. В таблице 3 приведены примеры средств IT-контроля, используемых для реагирования на риск, возникающий в процессе управления доступом [Будущее кибербезопасности ...].

Наличие IT-контролей позволит обеспечить высокий уровень целостности, доступности и конфиденциальности данных, надежность IT-операций и сохранность критически важной информации для компании.

Следует отметить, что для эффективного построения в компании системы разделения полномочий необходимо создать условия для внедрения, такие как: наличие устоявшихся бизнес-процессов, поддержка и вовлечение владельца бизнес-процесса, открытое взаимодействие с бизнес-экспертами и ключевыми пользователями информационных систем. Активное участие координаторов бизнес-процессов, которые, как правило, курируют функционирование информационных систем по направлению деятельности, позволит сократить ресурсы при определении конфликтующих ролей, идентификации рисков, построении матриц SoD. Сотрудничество заинтересованных сторон, таких как: ИТ-подразделение, отдел кадров, отдел информационной безопасности, владельцы ресурсов, позволит принять эффективные совместные решения о распределении полномочий (ролей). Тем самым будут исключены ошибки, нарушения и злоупотребления, а также задержки в обработке данных.

Таблица 3. **Примеры средств контроля для своевременного реагирования на риски, связанные с процессом управления доступом**

Table 3. **Examples of controls to respond in a timely manner to risks associated with the access management process**

IT-процесс	Риски	Средства IT-контроля
Управление доступом	Пользователи имеют права доступа, превышающие уровень, необходимый для выполнения порученных им обязанностей, что может стать причиной ненадлежащего разделения должностных обязанностей	Руководство утверждает характер и объем пользовательских прав доступа для нового и измененного доступа пользователей, включая стандартное применение профилей / ролей, важные операции по составлению финансовой отчетности и разделение обязанностей
		На основании матрицы SoD происходит проверка ролей и полномочий при подключении пользователей на предмет наличия конфликта полномочий. Проверка может проводиться координатором информационной системы при подключении пользователей и назначении ролей вручную или же автоматически, что существенно упростит процесс
		Доступ уволенных или переведенных пользователей своевременно удаляется или изменяется
		Пользовательский доступ (подключенные пользователи, состав их ролей) периодически проверяется координатором информационной системы
		Осуществляется мониторинг разделения должностных обязанностей, при этом права доступа, которые приводят к возникновению конфликта, либо удаляются, либо привязываются к компенсирующим средствам контроля, что документируется и тестируется
		Привилегированные права доступа (например, администраторы конфигурации, данных и безопасности) авторизованы и надлежащим образом ограничены

Примечание. Составлено авторами по результатам проведенных исследований.

Выводы

Таким образом, IT-аудит является активно развивающимся направлением внутреннего аудита, которое позволяет провести оценку эффективности информационных технологий и программного обеспечения, а также рассмотреть IT-систему со стороны рисков информационной безопасности, реализация которых может повлиять на деятельность организации на всех уровнях контроля. Аудит распределения прав доступа к информационным системам, как одна из составляющих IT-аудита, является интересным направлением для работы внутренних аудиторов, поскольку преднамеренное наделение пользователей излишними ролями может привести к созданию уязвимостей в системе управления рисками и внутреннего контроля, в том числе связанных с вероятной компрометацией данных, проведением мошеннических операций, совершением ошибок и т. д.

В целях исключения конфликтов полномочий при эксплуатации информационных систем необходимо выстроить систему разделения полномочий (SoD). В качестве одной из лучших практик по внедрению системы разделения обязанностей является создание SoD-матрицы, основная цель которой заключается в минимизации вероятности наступления рисков мошенничества, ошибок или действий, представляющих собой угрозу для организации. Наличие подобной IT-контроли позволит обеспечить целостность, доступность и конфиденциальность данных. Следует отметить, что механизм разделения полномочий будет работать наиболее эффективно в случае внедрения превентивных автоматизированных средств контроля, что впоследствии позволит минимизировать время и затраты на аудит.

СПИСОК ЛИТЕРАТУРЫ

Будущее кибербезопасности во внутреннем аудите. – URL: https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf

Кашин, Д. Аудит оценки качества данных в информационной системе / Д. Кашин, Н. Белых // Внутренний аудитор. – 2022. – № 3 (19). – С. 23–32.

Каширская, Л. В. Объекты аудита информационной безопасности и направления их проверки / Л. В. Каширская, Ю. А. Зурнаджьянц // Аудитор. – 2022. – № 1. – С. 21–31.

Кеворкова, Ж. А. Методические аспекты IT-аудита как инструмента повышения эффективности внутреннего контроля / Ж. А. Кеворкова // Аудитор. – 2021. – № 1. – С. 25–29.

Колодяжный, А. ИТ-аудит: анализ базовых процессов эксплуатации ИТ-инфраструктуры / А. Колодяжный // Внутренний аудитор. – 2021. – № 2 (14). – С. 49–54.

Международные основы профессиональной практики внутреннего аудита. Дополнительные руководства. Оценка риска кибербезопасности. Роли трех линий защиты. – URL: https://www.iia-ru.ru/upload/documents/professional_practice/practice_advisories/Implementation%20guides.%20Full%20set%202019.pdf

Нагаева, А. Методика проведения ИТ-проверки в части оценки использования внедренной ИС на примере промышленной компании. Обзорный документ / А. Нагаева, Д. Кашин, Н. Белых. – URL: https://www.iia-ru.ru/upload/inner-auditor/articles/2023_12%20IVA_IS_assessment.pdf

Сафонова, М. Ф. Аудит информационной и кибербезопасности: нормативное регулирование и проблемы функционирования / М. Ф. Сафонова, Д. Н. Кривошей // Международный бухгалтерский учет. – 2024. – № 6. – С. 644–664.

Суслова, П. Управление рисками, связанными с реализацией конфликта интересов / П. Суслова, Г. Бережной // Внутренний аудитор. – 2023. – № 4 (24). – С. 56–63.

Черноусов, И. Тайное познание: число утечек информации в мире выросло в 2,4 раз. Известия.iz. Интернет и технологии / И. Черноусов. – URL: https://iz.ru/1563836/ivan-chernousov/tainoe-poznanie-chislo-utechek-informatcii-v-mire-vyroslo-v-24-raza

REFERENCES

Budushhee kiberbezopasnosti vo vnutrennem audite [Future of Cybersecurity in Internal Audit]. URL: https://www.crowe.com/-/media/Crowe/LLP/folio-pdf/The-Future-of-Cybersecurity-in-IA-RISK-18000-002A-update.pdf

Kashin D., Belyh N. Audit ocenki kachestva dannyh v informacionnoj sisteme [Audit of Data Quality Assessment in the Information System]. *Vnutrennij auditor*, 2022, no. 3 (19), pp. 23-32.

Kashirskaja L.V., Zurnadzhjanc Ju.A. Obekty audita informacionnoj bezopasnosti i napravlenija ih

proverki [Objects of Information Security Audit and Directions of Their Verification]. *Auditor*, 2022, no. 1, pp. 21-31.

Kevorkova Zh.A. Metodicheskie aspekty IT-audita kak instrumenta povyshenija effektivnosti vnutrennego kontrolja [Methodological Aspects of IT Audit as a Tool for Increasing the Efficiency of Internal Control]. *Auditor*, 2021, no. 1, pp. 25-29.

Kolodjazhnyj A. IT-audit: analiz bazovyh processov jekspluatacii IT-infrastruktury [IT Audit: Analysis of Basic Processes of IT Infrastructure Operation]. *Vnutrennij auditor*, 2021, no. 2 (14), pp. 49-54.

Mezhdunarodnye osnovy professionalnoj praktiki vnutrennego audita. Dopolnitelnye rukovodstva. Ocenka riska kiberbezopasnosti. Roli treh linij zashhity [International Framework for the Professional Practice of Internal Auditing. Supplementary Guidelines. Assessing Cybersecurity Risk. Roles of the Three Lines of Defense]. URL: https://www.iia-ru.ru/upload/documents/professional_practice/practice_advisories/Implementation%20guides.%20Full%20set%202019.pdf

Nagaeva A., Kashin D., Belyh N. *Metodika provedenija IT-proverki v chasti ocenki ispolzovanija vnedrennoj IS na primere promyshlennoj kompanii. Obzornyj dokument* [Methodology of Conducting IT Audit in Terms of Assessing the Use of the Implemented Information System Using the Example of an Industrial Company. Review Document]. URL: https://www.iia-ru.ru/upload/inner-auditor/articles/2023_12%20IVA_IS_assessment.pdf

Safonova M.F., Krivoshej D.N. Audit informacionnoj i kiberbezopasnosti: normativnoe regulirovanie i problemy funkcionirovanija [Information and Cybersecurity Audit: Regulatory Framework and Operational Issues]. *Mezhdunarodnyj buhgalterskij uchet*, 2024, no. 6, pp. 644-664.

Suslova P., Berezhnoj G. Upravlenie riskami, svjazannymi s realizaciej konflikta interesov [Managing the Risks Associated with the Implementation of Conflicts of Interest]. *Vnutrennij auditor*, 2023, no. 4 (24), pp. 56-63.

Chernousov I. *Tajnoe poznanie: chislo utechek informacii v mire vyroslo v 2,4 raz. Izvestija.iz. Internet i tehnologii* [Secret Knowledge: Number of Information Leaks in the World Has Increased by 2.4 Times. Izvestia.iz. Internet and Technologies]. URL: https://iz.ru/1563836/ivan-chernousov/tainoe-poznanie-chislo-utechek-informatcii-v-mire-vyroslo-v-24-raza

Information About the Authors

Salavat D. Daudov, Head of the Department of Internal Audit, OOO Gazprom Dobycha Astrakhan, Lenina St, 30, 414000 Astrakhan, Russian Federation, sdaud@astrakhan-dobycha.gazprom.ru, https://orcid.org/0009-0006-8272-7992

Adelia M. Duisalieva, Auditor, Department of Internal Audit, OOO Gazprom Dobycha Astrakhan, Lenina St, 30, 414000 Astrakhan, Russian Federation, aduysalieva@astrakhan-dobycha.gazprom.ru, https://orcid.org/0009-0004-8976-7917

Информация об авторах

Салават Джигангирович Даудов, начальник отдела внутреннего аудита, ООО «Газпром добыча Астрахань», ул. Ленина, 30, 414000 г. Астрахань, Российская Федерация, sdaud@astrakhan-dobycha.gazprom.ru, https://orcid.org/0009-0006-8272-7992

Аделя Мадиевна Дуйсалиева, аудитор отдела внутреннего аудита, ООО «Газпром добыча Астрахань», ул. Ленина, 30, 414000 г. Астрахань, Российская Федерация, aduysalieva@astrakhan-dobycha.gazprom.ru, https://orcid.org/0009-0004-8976-7917