МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»
Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки, специальности)

Управление корпоративными информационными процессами
(направленность (профиль)

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему «Методы и инструменты аудита информационных технологий»

Студент М.Ю. Чехлов
(И.О. Фамилия) (личная подпись)

Научный руководитель к. п. н., доцент, Е.А. Ерофеева
(ученая степень, звание, И.О. Фамилия)

Тольятти 2022

Содержание

Введение

Мировые экономические системы оказались глобально взаимозависимыми и взаимосвязанными.

Информационные технологии пронизывают все сферы деятельности общества. Невозможно себе представить крупную корпорацию, где информационные технологии не оказывали бы критического влияния, не становились одним из стратегических направлений деятельности компаний.

Современный рынок насыщен программным обеспечением и оборудованием. Многие компании стоят перед выбором – заменить устаревающее ИТ-оборудование и софт, или модернизировать его.

Информация становится критически важным ресурсом организации. Все больше денежных средств и усилий уделяется на ее защиту от утечки, искажения, нарушения целостности.

В современном мире очень важным аспектом является доступность информации, непрерывность ИТ-процессов, все большую роль играют средства коммуникации.

ИТ-бюджеты занимают существенную часть в бюджетах крупных организаций. Понять необходимость вкладывания средств в крупные ИТ-проекты, эффективность их внедрения, окупаемость, может только специалист, владеющий как достаточным пониманием ИТ-технологий, так и аналитическими методиками, являющимися неотъемлемой частью дисциплины аудит информационных технологий (ИТ-аудит) [1].

Применение новых цифровых технологий дает значительные преимущества в деятельности компаний, и в то же время создает предпосылки для хищения, утраты, подделки, уничтожения, и блокирования информации, что приводит к нанесению экономического, репутационного или иного ущерба.

Особенно четко зависимость современного бизнеса от ИТ-технологий показала недавняя пандемия COVID-19

В соответствии с докладом Международного торгового центра (Centre du commerce international (CCI)) от 22 июня 2020 года, из-за глобального сбоя производственно-сбытовых цепочек мировая экономика потеряла по меньшей мере 126 миллиардов долларов [2]. Согласно ежегодному докладу бизнес-омбудсмена Бориса Титова, пандемия COVID-19 в России затронула более 4 млн компаний и ИП из общего числа 6 млн. То есть пострадали до 67% малых, средних и крупных предприятий, а также индивидуальных предпринимателей. 30 марта 2020 года в Москве был объявлен локдаун. И ИТ-специалисты множества компаний оказались перед рядом следующих вопросов:

- Как обеспечить удаленную работу большого количества специалистов, в том числе если они не имеют своего домашнего оборудования для выхода в интернет
- Что делать в случае, если внезапно пропадает связь с серверами
- Как перераспределить нагрузку на сервера, чтобы они сохраняли максимальную работоспособность и производительность
- Как обеспечить информационную безопасность конфиденциальной информации в условиях удаленной работы [13].
- Как обеспечить техническую поддержку пользователей 24x7

Для обеспечения бесперебойной работы, минимизации затрат и повышения конкурентного преимущества, менеджмент компаний начинает задаваться вопросами - кто может:

- оценить, насколько ИТ стратегия соответствует общей стратегии компании
- обеспечить независимую оценку имеющихся ИТ-процессов компаний
- идентифицировать и оценить ИТ-риски
- оценить эффективность внедряемых ИТ-проектов

Актуальность темы «Методы и инструменты аудита информационных технологий» обуславливает тот факт, что спектр угроз для ИС расширился. Это обусловлено передачей информации по общим сетям WiFi, «информационными войнами» конкурентов, большой текучкой специалистов. По данным западных аналитических агентств, до 95% попыток

несанкционированного доступа к закрытой информации происходит по инициативе бывших работников компаний. Проведение аудита позволяет проанализировать состояние безопасности функционирования информационных систем, определить риски с целью последующего управления ими.

После проведения аудита информационные системы компаний становятся прозрачными даже для не владеющих специализированной, выявляются основные риски бизнес-процессов, вырабатываются рекомендации по повышению эффективности функционирования ИТ-систем и т. д.

В то же время возникает вопрос как о построении качественной методологии самого ИТ-аудита, так и об инструментах, позволяющих внедрить данную методологию, автоматизировать работу самого ИТ-аудитора.

Для решения подобной задачи может потребоваться комплексное решение позволяющее автоматизировать процесс внутреннего аудита, начиная с описания бизнес-процессов, годового планирования и проведения аудиторской проверки и заканчивая мониторингом исполнения мероприятий по результатам аудита, а также обмениваться информацией с иными подразделениями осуществляющими ряд мероприятий по минимизации рисков компании, так называемыми подразделениями второй линии защиты (подразделения по управлению рисками, внутреннего контроля, информационной безопасности и т.д.).

Одной из наиболее популярных концепций позволяющей реализовать все вышеизложенное является концепция GRC-системы.

Концепция GRC говорит о том, что компоненты аудита, рисков, контролей и непрерывности бизнеса тесно связаны между собой и находятся в постоянном взаимодействии и подразумевает ведение бизнеса, основанное на системности и риск-ориентированном подходе. Согласно данной концепции GRC-система представляет собой интегрированный и целостный

подход к организации корпоративного управления, управления рисками и внутреннего контроля, позволяющий убедиться в том, что компания действует соответствующим образом, в пределах своего риск-аппетита, и представляет собой взаимосвязь стратегии, процессов, технологий и человеческих ресурсов, повышая эффективность и результативность деятельности.

Целью данной работы является анализ методов и инструментов внутреннего аудита информационных технологий на примере логистической компании ООО «City Plus», включающий в себя в том числе поиск технического решения, позволяющего автоматизировать, оптимизировать и повысить эффективность процесса аудита.

Задачи данной работы:

- проанализировать методы и инструменты проведения внутреннего аудита информационных технологий ООО «City Plus»;

- выбрать методологию оптимизации деятельности подразделения аудита информационных технологий, интеграцию модуля программного обеспечения для проведения внутреннего аудита с модулями подразделений второй линии защиты

- разработать технологию оптимизации внутреннего аудита информационных технологий компании за счет автоматизации и интеграции;

- протестировать разработанную технологию внутреннего аудита информационных технологий, а также оценить эффективность результатов тестирования.

Объектом исследования в работе выступает дистрибьютерская компания ООО «City Plus».

Предметом исследования в работе является процесс проведения аудита информационных технологий.

Научная новизна работы состоит в технологические решения для повышения эффективности процесса внутреннего аудита информационных технологий, позволяющего не ограничиваться рамками одного лишь подразделения ИТ-аудита. Компоненты аудита, рисков, контролей и

непрерывности бизнеса, владельцами которых могут быть иные подразделения компании (так называемая вторая линия защиты) тесно связаны между собой и находятся в постоянном взаимодействии, что подразумевает ведение бизнеса, основанное на системности, процессном и риск-ориентированном подходе. Используемое для этих целей автоматизированное решение GRC представляет собой интегрированный и целостный подход к организации корпоративного управления, управления рисками и внутреннего контроля, который позволяет убедиться в том, что компания достигает поставленных перед ней целей, минимизируя до приемлемого уровня присущие ей риски.

Гипотеза исследования. Предполагается, что если систематизировать процесс аудита информационных технологий путем создания единой базы по рискам, контролям и реализовавшимся инцидентам для ИТ-аудиторов и подразделений второй линии защиты (подразделения по управлению рисками, подразделения информационной безопасности), автоматизировать методы работы аудиторов, применяя инструменты GRC-системы, то это повлияет на эффективность работы подразделения внутреннего аудита, позволит сократить время на сбор и анализ информации по рискам, контролям, инцидентам и бизнес-процессам организации, стандартизирует и упорядочит работу аудиторов, позволит наладить более тесную коммуникацию с представителями объектов аудита.

Методы исследования. При проведении исследования настоящей темы использовались методы анализа и синтеза, наблюдения, сравнения, визуализации, бенчмаркинга (сравнения с лучшими практиками), метод описания и изложения.

Теоретическая значимость результатов исследования состоит в следующем:

Исследование позволит актуализировать информацию, уже имеющуюся по рассматриваемому вопросу, а также привнести ряд новых моментов в уже имеющуюся базу знаний, расширить теоретическое описание предмета

исследования., проанализировать и систематизировать новые данные по исследуемому вопросу, послужит стимулом повышения общетеоретического уровня современных исследований в области аудита информационных технологий.

Практическая значимость результатов исследования:

В настоящее время крупными компаниями востребовано решение по автоматизации внутреннего аудита информационных технологий, позволяющее оптимизировать процесс внутреннего аудита, за счет использования средств контроля за работой аудиторов, упорядочения их работы использования информации получаемую от иных подразделений занимающихся минимизацией рисков организации в качестве единой базы знаний. Практическая ценность работы состоит в оптимизации работы подразделения внутреннего аудита информационных технологий, стандартизации и шаблонизации работы ИТ-аудиторов, сокращению времени на получение необходимой информации, повышении качества годового планирования внутренних аудитов, повышении эффективности исполнения мероприятий по результатам аудитов.

Структура работы представлена введением, четырьмя главами, заключением и списком использованных источников.

1. Методы и инструменты аудита информационных технологий

1.1. Анализ деятельности ООО «City Plus»

ООО «City Plus» (далее – Компания) является дистрибьютерской компанией по реализации ряда пищевых продуктов и напитков

Компания была основана в 1995 году и реорганизована в ОО в 2001 году.

Основными направлениями деятельности Компании являются:

- оптовая торговля продовольственными товарами (продажи pre-sale и van-sale);
- логистические услуги.

Основными партнерами Компании являются представители фирм Европы и Японии, производящих и реализующих продовольственные товары в широком ассортименте.

Организационная Структура Компании.

Компания является обществом с ограниченной ответственностью.

Вид основной деятельности предприятия: логистические услуги.

Общее количество работников предприятия – 15 тысяч человек.

Количество филиалов: 17

Ключевые должности Компании:

- Генеральный директор;
- Заместитель Генерального директора по продажам;
- Заместитель Генерального директора по управлению и обеспечению;
- Заместитель Генерального директора по финансам;
- Директор по логистике;
- Директор по маркетингу и сбыту.

Структура должностей указана на рисунке 1

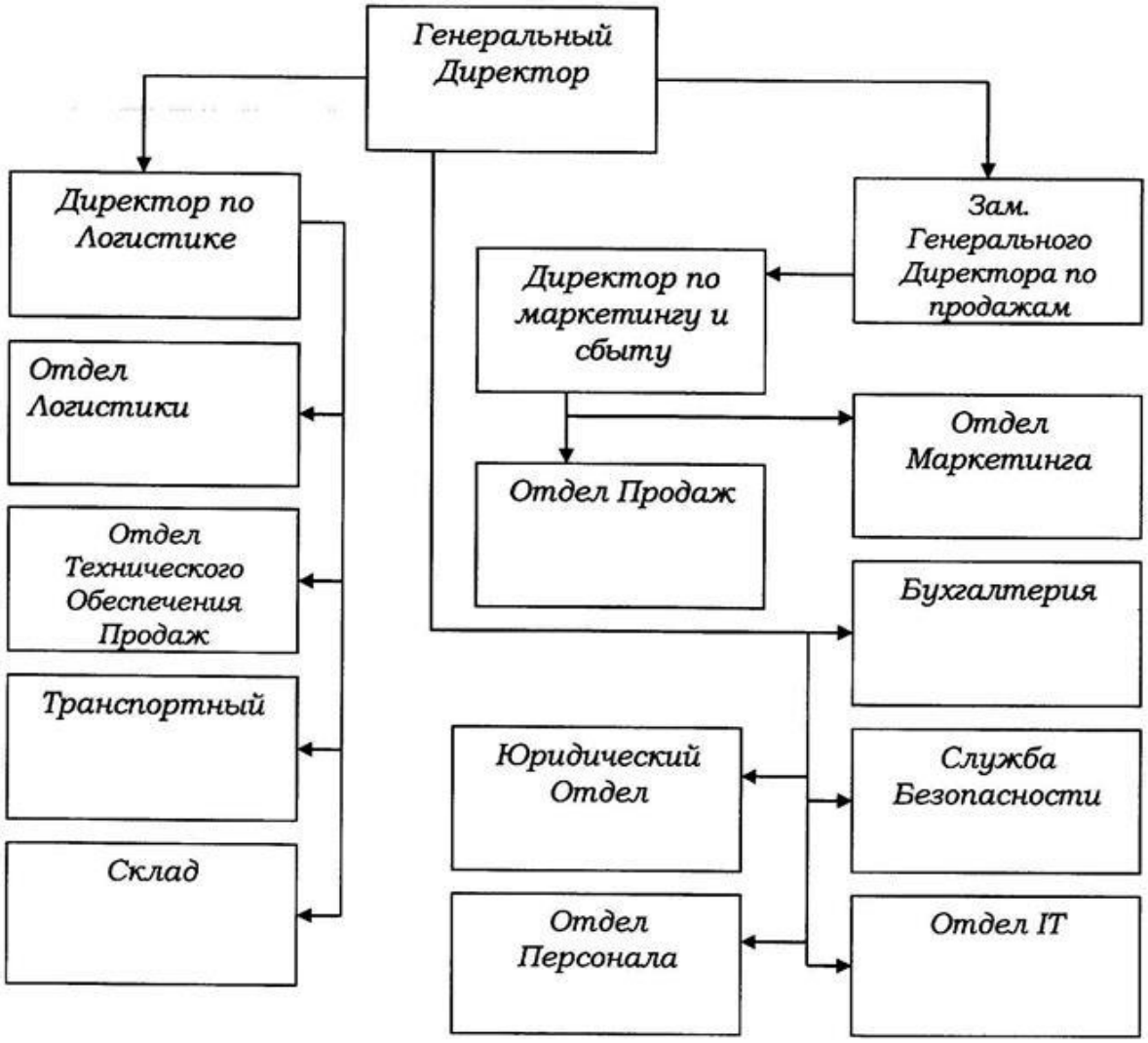


Рисунок 1 – Структура должностей

Процессы Компании могут быть сгруппированы по 5 блокам:

- Планирование распределения
- Управления запасами
- Управление складами
- Отгрузка и транспортировка
- Пополнение запасов

Декомпозиция блоков указана на рисунке 2

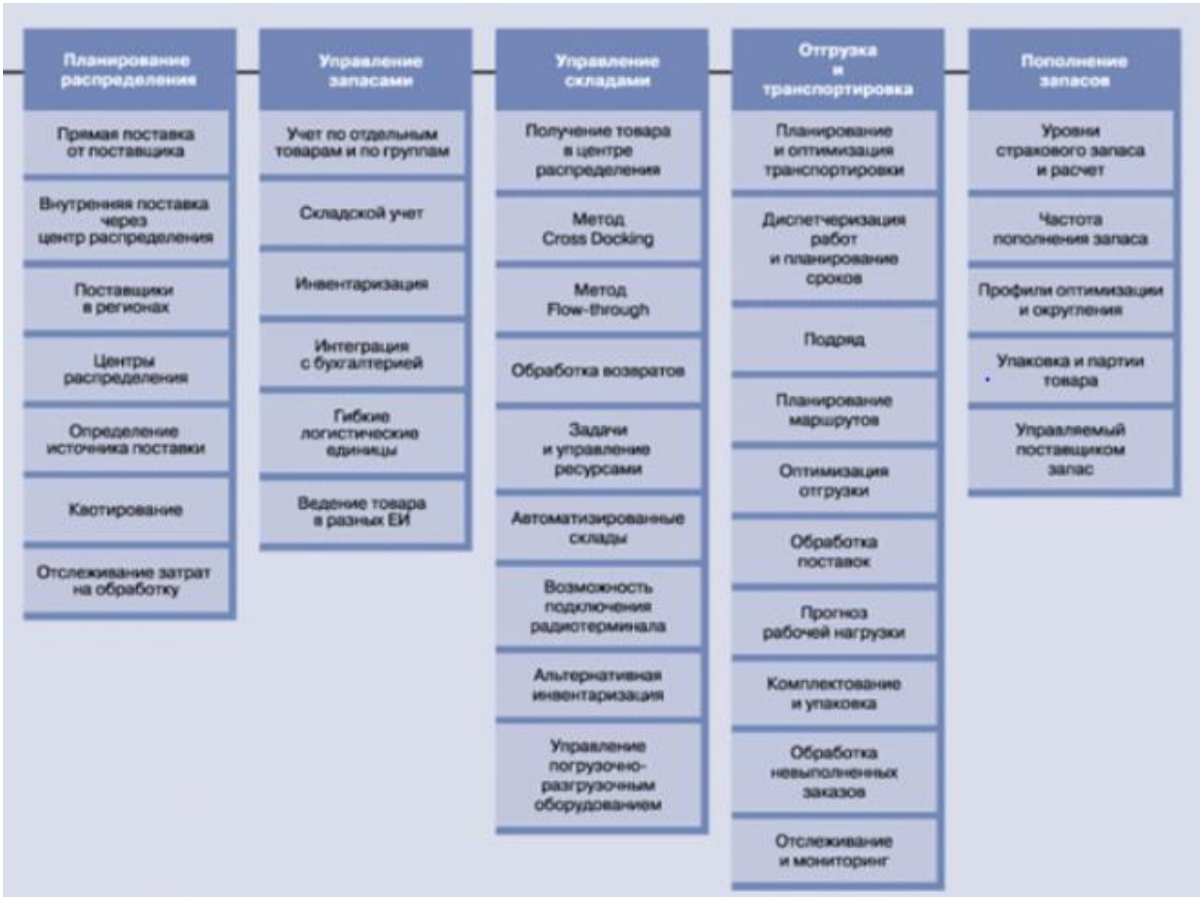


Рисунок 2 – Декомпозиция блоков

Основные этапы закупочного и реализационного циклов Компании представляют из себя следующее:

- Проведение мониторинга потребительского рынка;

Для проведения мониторинга используются данные, полученные отделом аналитики продаж (исторические данные, анализ конкурентов, полученный из специализированных источников, внешние обзоры);

- Составление бюджета на закупку/бюджета продаж;

На основании полученных данных отделом финансового планирования составляются бюджеты продаж, которые содержат следующую информацию:

– статьи доходов

– статьи расходов

– данные о количестве закупаемой и реализуемой продукции

– данные о валовой и чистой прибыли

- Выбор поставщика;

Выбор поставщика осуществляется путем запроса коммерческих предложений. Сотрудниками отдела анализа цен собирается и анализируется информация о сроках поставки и наиболее оптимальных ценах.

- Заключение договоров с поставщиками;

Все договоры с поставщиками согласовываются рядом подразделений Компании – юридической службой, закупочной службой, службой безопасности, службой финансового контроллинга.

- Оплата заказа;

Оплата заказа обычно осуществляется на условиях предоплаты. Для осуществления оплаты необходим ряд следующих документов:

- Инвойс от поставщика;
- Копия договора с поставщиком;
- Платежное поручение
- Приемка товара на склад (рисунок 3)
- Заключение договоров с покупателями;

Заключение договоров также проверяется рядом подразделений, в том управлением финансового планирования

- Отправка товара со склада.

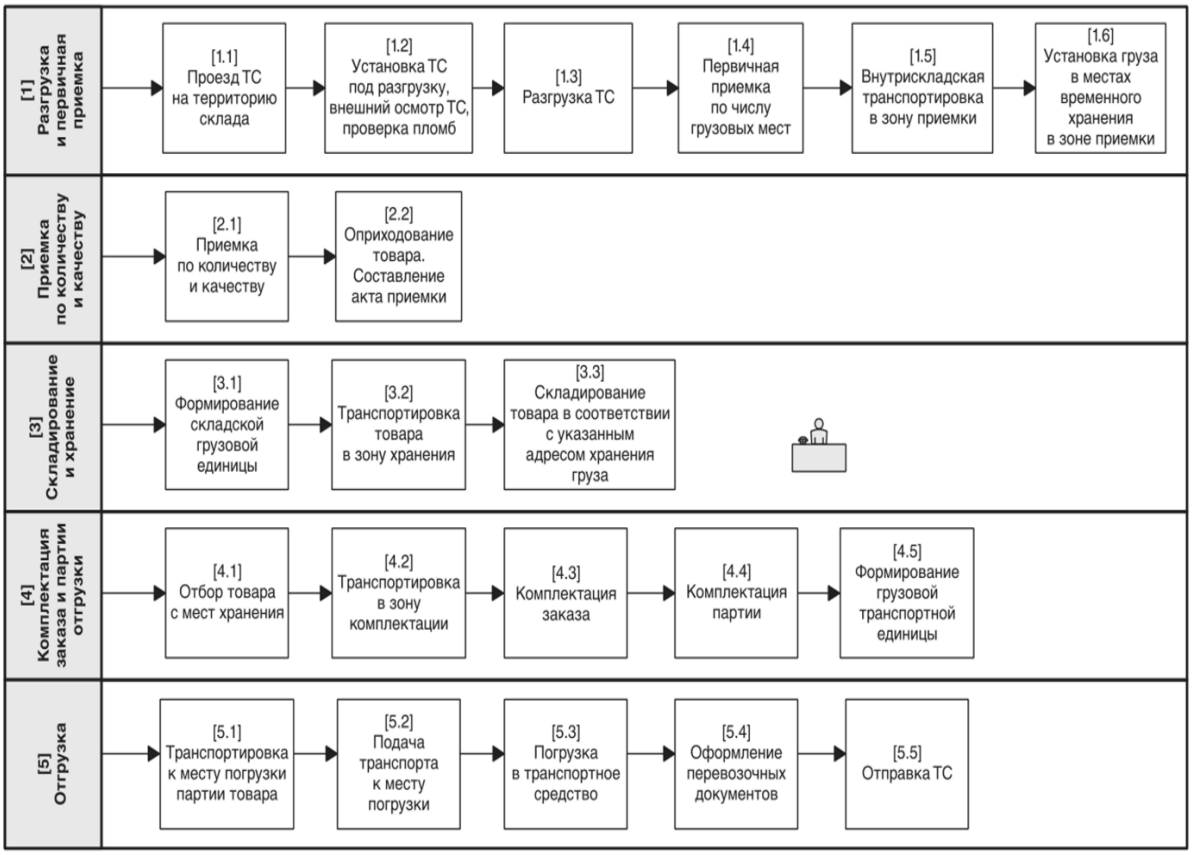


Рисунок 3 – Приемка товара на склад

Основные виды документооборота:

- Служебные записки. Формируются в СЭД Директум согласно установленных шаблонов;
- Приказы. Формируются посредством текстового редактора, сканируются в формат pdf и заверяются электронной подписью, после чего согласуются посредством СЭД «Директум»;
- Листы согласования. Формируются автоматически в СЭД Директум;
- Переписка с государственными органами. Оформляются на официальных бланках предприятия. Отправляются посредством обычной почты или приложения MS Outlook;
- Переписка с поставщиками и подрядчиками. В основном – переписка посредством MS Outlook;

- Переписка с клиентами. В основном – переписка посредством MS Outlook;
- «Горячая линия». Получение жалоб о некорректных или противоправных действиях посредством формы на сайте.;
- Финансовая и управленческая отчетность. Различие формы пакета MS Office. Отправка преимущественно посредством MS Outlook. Существенная информация шифруется с помощью системы ассиметричных ключей.

Информация является одним из ключевых активов организации.

Поэтому эффективное функционирование информационных потоков является жизненно важным условием для выживания организации в современных условиях. Учитывая ситуацию с пандемией, в том числе зависимость от стабильной работы информационных систем в условиях удаленной работы, быстрота восстановления информационных систем, а также оперативная работа технической поддержки являются процессами первой приоритетности.

Основными информационными системами Компании являются следующие:

- Стандартный набор Windows, MS Office
- SAP – поддерживает модули по финансам, закупке и продажам, проектам, ремонтам, а также вопросы кадрового учета. Указанная система имеет классическую трехуровневую структуру [11].

Презентационный уровень – позволяет осуществлять диалог с пользователем, ввод и вывод данных, посредством интерфейса SAP GUI (Graphical User Interface)

Уровень приложений – позволяющий обрабатывать информацию в соответствии с заданными правилами бизнеса, формировать служебные функции для доступа к базе данных. Рабочие процессы могут быть распределены по различным серверам. Управление рабочими процессами обеспечивает специальный диспетчер:

Уровень данных – имеет место реляционная система управления базами данных (РСУБД). Работа архитектуры SAP основана на понятии транзакции – целостная последовательность действий, которая либо осуществляется полностью, либо не осуществляется вовсе. 1С: Предприятие версия 8.2 (рисунок 4) – позволяет вести учет основных средств и заработной платы. Модуль кадрового учета системы SAP интегрирован с модулем по учету заработной платы 1С [4].

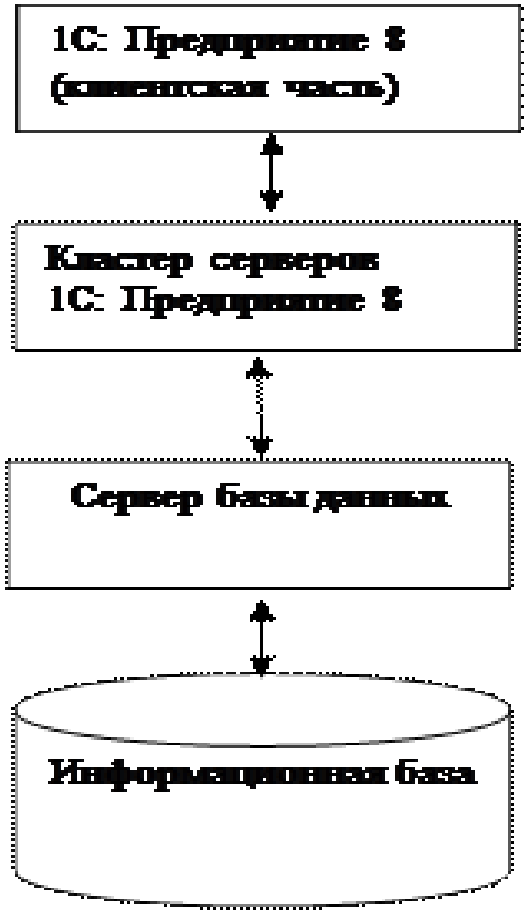


Рисунок 4 – Архитектура 1С

СЭД Директум (рисунок 5) – система электронного документооборота Компании. Данная система интегрирована с ресурсом MS SharePoint, а также с почтовым сервером MS Outlook (рисунок 6).

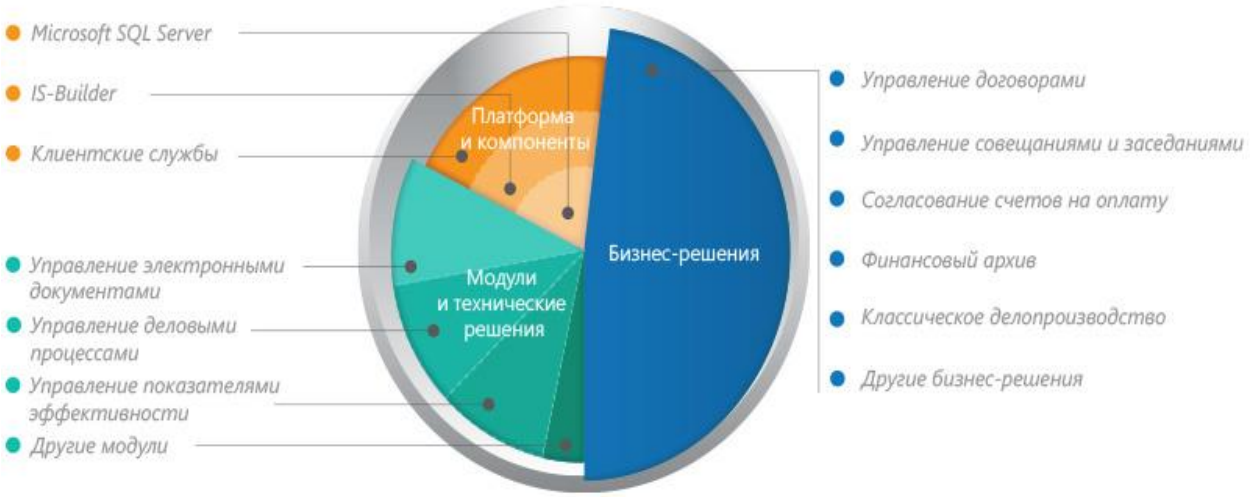


Рисунок 5 – Архитектура СЭД

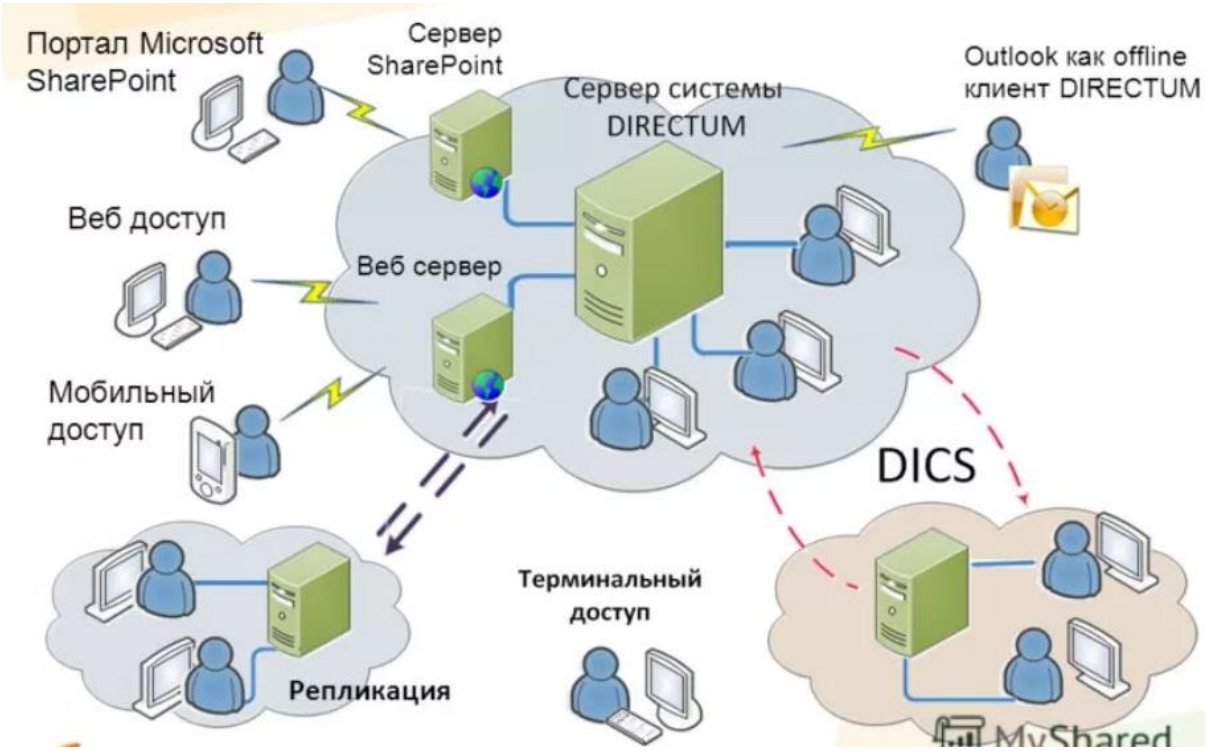


Рисунок 6 – Интеграция СЭД

Acronis Backup – система по управлению резервным копированием. CRM система (рисунок 7), позволяющая управлять процессами работы с клиентами.

Рисунок 7 – CRM система

DLP (Data Leaks Prevention) система «Контур информационной безопасности» – система предотвращающая утечку данных (рисунок 8).

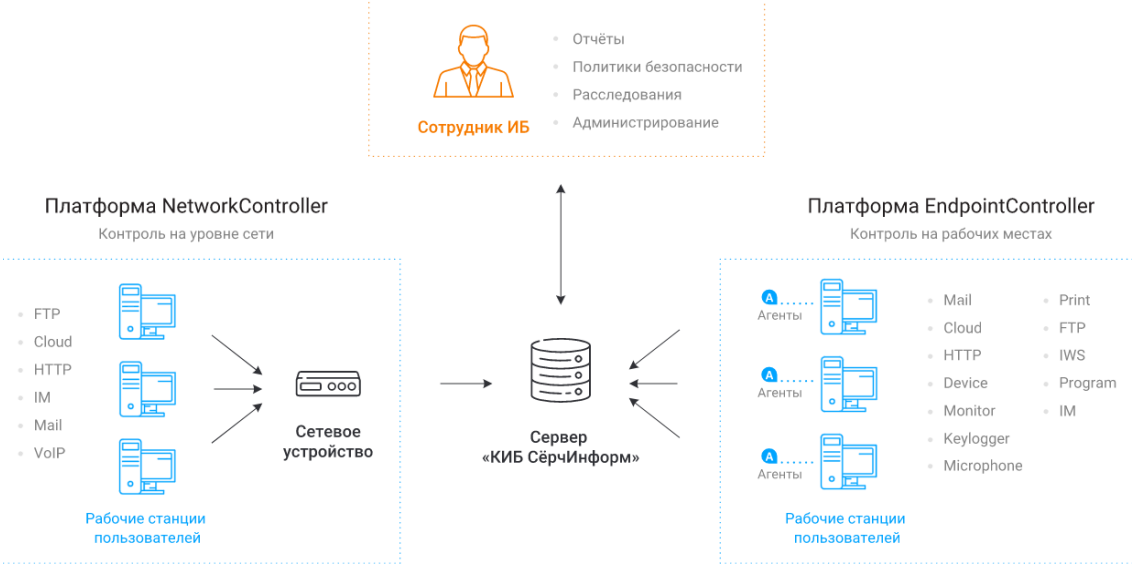


Рисунок 8 – Архитектура DLP-системы

Внедрение новых информационных систем, а также развитие старых помогает Компании получить конкурентное преимущество, укрепиться на рынке, максимизировать свою прибыль.

Неправильное использование информационных систем, отсутствие их защищенности от внешних и внутренних угроз, отсутствие контроля за их внедрением может привести к реализации рисков, ведущих в свою очередь к тому, что Компания понесет убытки [3].

Существуют следующие требования бизнеса к работе информационных систем (таблица 1):

Таблица 1 – Требования бизнеса к работе информационных систем

Результативность	информация предоставлена своевременно, корректно и в виде, пригодном для использования
Эффективность	Информация предоставлена посредством оптимального использования ресурсов
Конфиденциальность	Информация защищена от несанкционированного доступа
Целостность	Информация защищена от несанкционированных изменений
Доступность	Информация доступна всегда, когда она необходима для целей и задач бизнеса
Соответствие требованиям	Соблюдаются законодательные и внутренние нормативные акты в отношении хранения, использования и распространения информации
Надежность и достоверность	Информация является надежной для принятия решений

1.2. Цели и методы аудита информационных технологий.

Целью аудита информационных технологий (ИТ-аудита) Компании является совершенствование системы, корпоративного управления, а также систем управления ИТ-рисками и системы внутреннего контроля за ИТ.

С этой целью, ИТ-аудиторы.

- участвуют в оценке ИТ-рисков;
- помогают подготавливать нормативные документы в области ИТ;
- помогают связать бизнес-риски и ИТ-риски;
- осуществляют проведение периодических аудитов;
- содействуют в правильной организации управления ИТ;
- осуществляют независимую оценку.

Этапы аудиторского цикла показаны на рисунке 9.

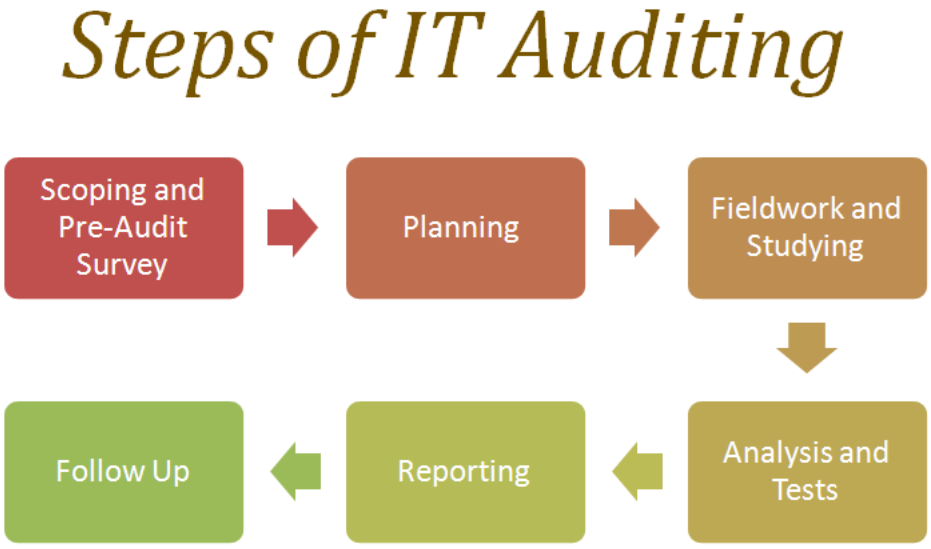


Рисунок 9 – Этапы аудиторского цикла

Области аудита информационных технологий могут быть следующими [25]:

- Процесс обеспечения непрерывности деятельности бизнеса;
- Информационная безопасность;
- Программирование и разработка ИТ-систем;
- Управление ИТ-портфелем и ИТ-проектами;
- Системное администрирование;
- Администрирование баз данных;

Международная ассоциация ИТ-аудиторов ISACA выделяет следующие домены знаний, необходимые для подготовки ИТ-аудиторов:

- Процесс аудита информационных систем;
- Корпоративное управление и ИТ-менеджмент;
- Приобретение, разработка и внедрение информационных систем;
- Поддержка информационных систем;
- Защита информационных активов.

Одной из наиболее наглядных иллюстраций этой профессии является концепция трех линий защиты (рисунок 10):

Рисунок 10 – Три линии защиты Компании

Как видно из приведенной схемы первую линию защиты формируют непосредственно сами структурные подразделения [14]. Они являются владельцами рисков и несут ответственность за выявление, управление, снижение уровня рисков, анализ и формирование отчетности по ключевым рискам. Руководители структурных подразделений обязаны разработать, внедрить и обеспечить функционирование контрольных процедур в бизнес-процессах, где они являются владельцами [10].

Во вторую линию о входят подразделения, ответственные за управление рисками, систему внутреннего контроля, безопасность, комплаенс, юридическое сопровождение и т. п. Они обеспечивают непрерывный мониторинг процесса разработки и функционирования контрольных процедур, относящихся к первой линии защиты,

Третью линию защиты представляет собой независимое подразделение, функционально подотчетное высшему руководству (например- Совету директоров). Оно проводит независимую оценку качества действующих процессов управления рисками, и внутреннего контроля, выявляет узкие места процессов, даёт предложения по совершенствованию системы корпоративного управления, управления рисками и внутреннего контроля. Совет директоров принимает это заключение как руководство к действию. Под надзором комитета по аудиту служба внутреннего аудита проводит мониторинг функций первой и второй линий защиты, а также осуществляет контроль выполнения корректирующих мероприятий.

Аудит не выстраивает систему управления рисками и внутреннего контроля, а лишь оценивает их эффективность [12]. В этом есть резон, так как в противном случае аудитору придется проверять то, что он построил сам. В этом случае возможно негативное влияние на независимость и объективность аудиторских суждений.

Одной из важных составляющих деятельности подразделения аудита информационных технологий является его взаимодействие с подразделениями второй линии защиты. Обмен информацией об идентифицированных

уязвимостях, рисках и контролях, произошедших инцидентах, повышает эффективность работы аудиторов, увеличивает ту ценность, которую они привносят в организацию.

При проведении высокоуровневого современного ИТ-аудита ключевым словом является слово - бизнес.

В первую очередь необходимо понимать, как цели ИТ-технологий соотносятся с целями организации, с ее стратегией (рисунок 11). Ведь ИТ служит для того, чтобы поддерживать бизнес, а не наоборот. Важно понимать – окупаются ли внедряемые ИТ-проекты, ведется ли управление ИТ-портфелем с должной эффективностью.

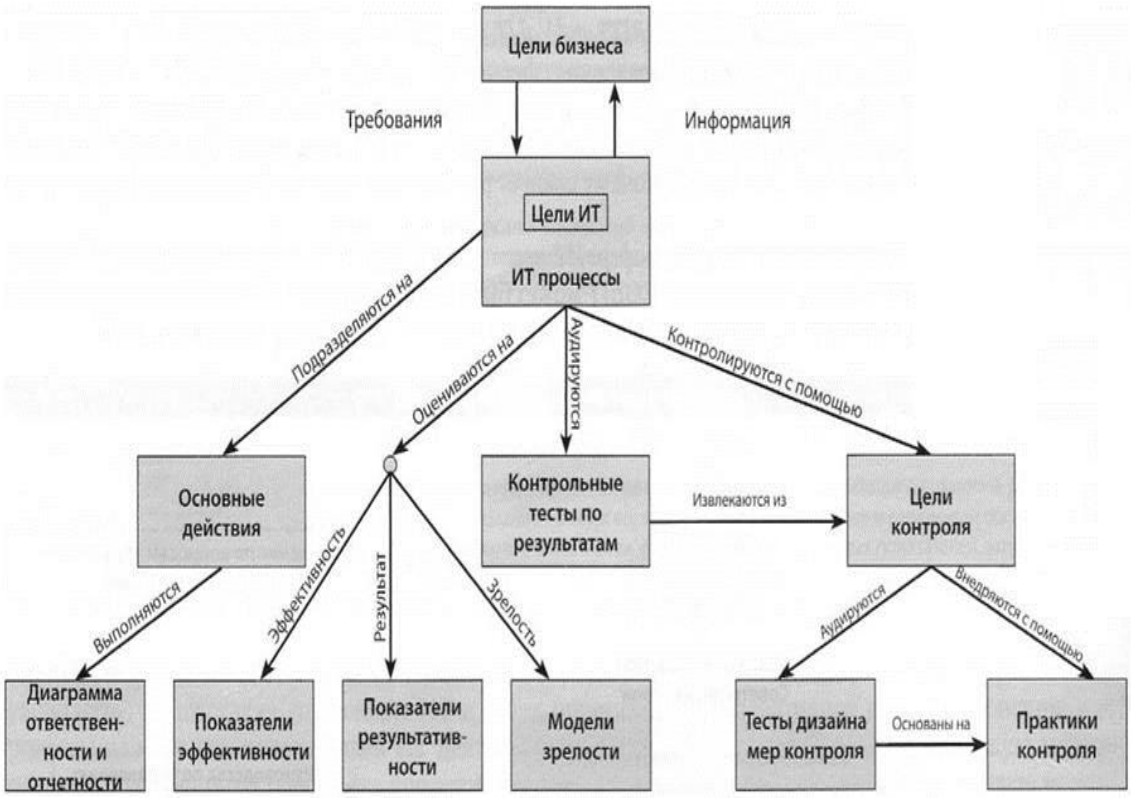


Рисунок 11 – Взаимосвязь целей бизнеса и ИТ

Двумя основополагающими понятиями для современного ИТ-аудита являются:

- Понятие процессного подхода в ИТ.

- Понятие риск-ориентированного подхода в ИТ.

Понятие процессного подхода в ИТ. Подход к организации и анализу деятельности компании, основанный на выделении и рассмотрении ее бизнес-процессов, каждый из которых протекает во взаимосвязи с другими бизнес-процессами компании или внешней средой. Подход начинается с рассмотрения процессов более высокого (стратегического) уровня и заканчивается обеспечивающими процессами организации [30].

На рисунке 12 показана схема процессной модели:

Рисунок 12 – Типовая модель процессов

Как уже говорилось бизнес-процессы — это совокупность взаимосвязанных мероприятий или работ, направленных на создание определённого продукта или услуги для потребителей

В эпоху цифровизации информационные технологии и информационные системы становятся важнейшими активами организации. Они несут в себе как добавление стоимости в организацию и

повышение конкурентного преимущества. Но также, они являются источников новых рисков, зачастую глобального масштаба.

В соответствии с определением Института внутренних аудиторов - внутренний аудит является деятельностью по предоставлению независимых и объективных гарантий и консультаций, направленной на совершенствование работы организации. Внутренний аудит помогает организации достичь поставленных целей, используя систематизированный и последовательный подход к оценке и повышению эффективности процессов управления рисками, контроля и корпоративного управления

При проведении проверок ИТ-аудитору может понадобиться, как понимание ИТ-рисков и связанных с ними контролей, так и понимание ряда ИТ-процессов на стратегическом, тактическом, операционном и технологическом уровне (рисунок 13). Например, таких процессов как:

- Управление ИТ-стратегией
- Закупка ПО и ИТ-услуг
- Разработка ПО
- Установка и обновление ПО
- Управление ИТ-инфраструктурой и коммуникациями
- Управление информационной безопасностью
- Управление ИТ-архитектурой;
- Управление доступностью;
- Управление изменениями;
- Управление мощностями;
- Управление инцидентами;
- Управление конфигурациями;
- Управление непрерывностью предоставления сервисов ИТ (непрерывностью бизнеса);
- Управление хранилищами данных;
- Управление удаленным доступом;
- Управление безопасностью;

- Управление финансами в сфере ИТ;
- Управление потоками информации.

Рисунок 13 – ИТ-процессы организации

Понятие риск-ориентированного подхода в ИТ. При проведении ИТ-аудита аудиторы Компании оперируют понятием рисков и контролей, так как на текущий момент имеет место тенденция смешения аудитов в сторону процессно-ориентированного и риск-ориентированного подходов [15]. Данную концепцию можно рассмотреть на примере стандарта COSO ERM (рисунок 14).

Данная концепция была разработана так называемым Комитетом организаций-спонсоров Комиссии Трейдуэя. Данная концепция включает в себя подходы к идентификации и оценки рисков организации, а также к способам их минимизации, в том числе и внутренним контролям.

Рисунок 14 – Модель COSO ERM

Модель COSO ERM. Модель COSO (а также аналогичные модели управления рисками, например, FERMA), применима к любым процессам организации. Рассмотрим ее элементы применительно к ИТ-аудиту.

Восемь компонентов модели. Внутренняя среда (Internal environment). Внутренняя среда представляет собой атмосферу в организации и определяет, каким образом риск воспринимается сотрудниками организации, и как они на него реагируют [29].

Внутренняя среда применительно к сфере ИТ включает в себя организационную структуру, внутренние документы, декларируемые ценности. При проведении аудита ИТ-аудитор должен понимать:

- место ИТ в структуре организации;
- уровень развития ИТ-процессов;
- имеется ли описание Ит-процессов;

- поддерживает ли руководство внедрение передовых практик в области ИТ (например, имеется ли Комитет по ИТ-инвестициям);
- этические ценности организации (насколько аудируемые процессы подвержены риску фрода).

Постановка целей (Objective setting). Цели должны быть определены до того, как руководство начнет выявлять события, которые потенциально могут оказать влияние на их достижение. Аудитору необходимо понимать:

- имеет ли руководство ИТ-подразделений четко определенные цели;
- соотносятся ли цели ИТ с бизнес-целями и стратегией организации;
- определены ли цели ИТ в количественных характеристиках (быстрота внедрения, допустимое время простоя, окупаемость, и т. д.).

Определение событий (Event identification). Внутренние и внешние события, оказывающие влияние на достижение целей, должны определяться с учётом их разделения на риски или возможности.

Аудитор должен понимать:

- определяет ли руководство ИТ события, которые могут негативно повлиять на достижение целей;
- классифицирует ли оно эти события в зависимости от источников возникновения.

В качестве примера такой классификации можно привести схему, указанную на рисунке 15:

Рисунок 15 – Пример классификации событий

Оценка рисков (Risk assessment). Риски анализируются с учётом вероятности их возникновения и влияния с целью определения того, какие действия в отношении них необходимо предпринять. Аудитору необходимо убедиться, что руководство ИТ проводит качественную или количественную оценку ИТ-рисков, и классифицирует их значимость в зависимости от вероятности возникновения и последствий рисков [26].

Реагирование на риск (Risk response). Руководство выбирает метод реагирования на риск — уклонение от риска, принятие, сокращение или перераспределение риска, — разрабатывая ряд мероприятий, которые позволяют привести выявленный риск в соответствие с допустимым уровнем риска.

Аудитору необходимо убедиться, что:

- руководство разрабатывает ряд мер для реагирования на имеющиеся риски;
- данные меры включают в себя в том числе и ИТ-контроли (физические и логические).

Средства контроля (Control activities). Политики и процедуры разработаны и установлены таким образом, чтобы обеспечивать «разумную» гарантию того, что реагирование на возникающий риск происходит эффективно и своевременно. Аудитору необходимо провести тестирование контролей и убедиться в их операционной эффективности. Примеры контролей указаны на рисунке 16.

Рисунок 16 – Примеры внутренних ИТ-контролей

Мониторинг (Monitoring). Весь процесс управления рисками организации отслеживается и по необходимости корректируется. Мониторинг осуществляется в рамках текущей деятельности руководства или путём проведения периодических оценок. Аудитору необходимо убедиться, что:

- существующий процесс оценки рисков является актуальным;
- новые риски выявляются и переоцениваются на периодической основе.

Макро и микроуровень ИТ-аудитов. Процесс аудита информационных систем Компании можно рассматривать как на макро, так и на микроуровне. Первым шагом является так называемое построение «Вселенной аудита» - модели ИТ-аудита, представляющей собой описание основных ИТ-процессов, имеющихся в организации [27].

Макроуровень– это уровень годового планирования. Имея понимание о критичности ИТ-систем и ИТ-процессов, наличии уязвимостей,

подверженности рискам, аудитор определяет наиболее критичные системы и процессы для организации. Именно эти системы и процессы попадут в годовой план аудита с наибольшей вероятностью.

Здесь имеет место так называемый риск-ориентированный подход – наиболее рисковые зоны должны быть покрыты первыми.

Для определения наиболее критичных систем и процессов аудитор должен ориентироваться как на мнение собственников и менеджмента Компании (путем проведения интервью, анкетирования, использования методик самооценки внутренних контролей), так и на собственное профессиональное суждение (например, использованием методики оценки информационных систем/процессов по риск-факторам) [28].

При классификации/оценке информационных систем/процессов может быть использована следующая классификация:

- Система/процесс не являются критическими для достижения целей организации
- Система/процесс могут привнести определенную добавленную стоимость в организацию, при условии серьезных капиталовложений
- Система/процесс приносит добавленную стоимость в организацию, при достаточной поддержке на текущем уровне
- Система/процесс являются чрезвычайно важными для достижения целей организации
- Система/процесс являются критическими. Остановка системы/процесса может привести к остановке основной деятельности организации.

Микроуровень – это уровень отдельного аудиторского задания.

Современные методы ИТ-аудита. Современные методы проведения ИТ-аудита обычно основываются на подходах организации ISACA (англ. Information Systems Audit and Control Association) являющейся общемировым объединением профессионалов в области аудита информационных технологий, риск менеджеров и специалистов по

информационной безопасности. Базой для проведения ИТ-аудитов служит методология COBIT.

COBIT (аббр. от англ. Control Objectives for Information and Related Technologies «Задачи управления для информационных и смежных технологий») — методология управления информационными технологиями, принадлежащая и разрабатываемая некоммерческой организацией ISACA (англ. Information Systems Audit and Control Association) [5]. Представляет собой пакет международных и национальных стандартов и руководств в области управления ИТ, ИТ аудита основанных на анализе и конвергенции существующих стандартов и ведущих практик в области управления ИТ.

Согласно методологии, COBIT процесс аудита информационных технологий состоит из следующих этапов:

Предварительное обследование: в рамках данного этапа определяются цели, и объем аудиторского задания, происходит ознакомление с объектом аудита, запрашивается техническая и иная документация по информационным системам и прочим ИТ-активам, анализируются ИТ-риски и ИТ-контроли [24].

Аудитор выбирает те контроли, которые он будет тестировать на эффективность и формирует список аудиторских процедур, которые следует выполнить для тестирования контролей.

При выполнении аудита могут использоваться следующие виды аудиторских процедур.

Наблюдение. Аудиторская процедура по наблюдению за людьми, или действиями, или процессами, при этом аудитор не участвует в процессе, а только описывает наблюдаемые действия. Наблюдение может проводиться, как в открытой форме (когда персонал осведомлен о том, что за его действиями наблюдают), так и в тайной форме (когда персонал не осведомлен о том, что за его действиями наблюдают) [6]. Пример: аудитору необходимо убедиться, что осуществляется достаточный видеоконтроль за помещением серверной. Он получает доступ к изображениям видеокамер и убеждается, что

изображение является четким, обзор камер фиксирует подходы и вход в серверное помещение

Повторное исполнение. Аудитор пытается самостоятельно выполнить действия аудируемых. Пример: Резервное копирование данных критической информационной системы осуществляется раз в день. Тестирование восстановления данных проводится ИТ-персоналом раз в три месяца. Аудитор пытается самостоятельно восстановить данные из резервной копии в тестовой системе, чтобы убедиться в эффективности процесса резервного копирования.

Инспектирование. Представляет собой изучение физического состояния материальных объектов или ресурсов. Выполняется для получения первичной информации об объекте аудита (пример: инспектирование ВНД на наличие контрольных процедур), а также для проверки уже имеющиеся информации (пример: проверка расходных кассовых документов на наличие подписей, инвентаризация основных средств). Аудитор осуществляет просмотр документов, транзакций, данных в информационных системах, с целью подтверждения или опровержения гипотезы. Пример: Аудитор просматривает журнал событий информационной системы с целью поиска следов неправомерных действий [23].

Интервью. Аудитор проводит беседу с аудируемыми или третьими лицами. Пример: аудитор проводит интервью с владельцем информационной системы, с целью получения информации о рисках присущих системе и ИТ-контролях направленных на минимизацию рисков.

Запрос. Аудитор запрашивает интересующую его информацию/документацию у аудируемых/третьих лиц. Запрос позволяет аудитору получить первоначальную информацию об объекте аудита.

Аудиторская процедура запрос бывает двух видов:

- Запрос в письменной форме, отправляемый персоналу объекту аудита, с получением ответа в письменной форме.

- Запрос в виде интервью в устной форме при личной встрече с персоналом объекта аудита или по телефону. В отличие от предыдущего запроса, получаемая информация заполняется непосредственно аудитором.

Пример: аудитор запрашивает матрицу полномочий у владельца информационной системы.

Бенчмаркинг. Эта процедура позволяет аудитору сравнить информацию об объекте аудита с лучшими практиками.

Аудиторская процедура бенчмаркинг бывает двух видов:

- Внутренний бенчмаркинг – сравнение деятельности одного объекта аудита с другим в рамках одной организации.

- Внешний бенчмаркинг – сравнение деятельности одного объекта аудита одной организации с объектом другой организации.

Разработка программы аудита (включающую аудиторские процедуры, сроки их выполнения и ответственных за выполнение [7].

Каждая из процедур должна быть направлена на подтверждение одного или нескольких следующих критериев:

- Достоверность – отсутствие существенных ошибок в информации.
- Соответствие - выражается в соответствии законам, требованиям, регулирующим актам и т.д.
- Эффективность - получение соответствующего результата посредством оптимального использования ресурсов.
- Действенность – показатель, характеризующий достижение наилучшего результата.
- Сохранность – защита информации и материальных активов от хищения.
- Производительность - показатель, характеризующий отношению объёма проделанной работы ко времени, за которое она была совершена.
- Прибыльность - показатель, характеризующий возможность или способность процесса принести прибыль.

- Своевременность – характеризует выполнение бизнес-процесса за определенный промежуток времени или к определенному моменту времени.
- Полезность – характеризует информацию как значимую и имеющую отношение к бизнес-процессу, а также получаемую регулярно, корректно, последовательно и в удобном виде.
- Доступность – имеет отношение к наличию информации, когда она необходима в бизнес-процессе.
- Результативность – характеризует направленность на определенный результат.
- Надежность – характеризует отсутствие сбоев или отказов в бизнес-процессе в течение определенного времени.
- Экономичность - характеризует условие, предполагающее, что затраты на обработку не должны превышать получаемый эффект.
- Конфиденциальность – защита информации от несанкционированного раскрытия.
- Целостность – точность, полнота и обоснованность информации.

Выполнение процедур, указанных в программе аудита. Целью выполнения аудиторских процедур является определение эффективности процессов/систем, поиск путей их улучшения, выявление рисков и уязвимостей, и путей их минимизации, а также тестирование эффективности ИТ-контролей.

Например, аудитору необходимо убедиться, что у всех уволенные сотрудников заблокированы учетные записи (контроль за блокировкой учетных записей). Аудитор выгружает список уволенных сотрудников и сопоставляет его посредством функции ВПР в MS Excel со списком сотрудников, имеющих активные учетные записи в информационной системе.

При проведении тестирования аудитор опирается на собранные посредством процедур аудиторские доказательства. Аудиторские доказательства должны быть достаточными и соответствующими.

Достаточность доказательств – является количественным измерителем аудиторских доказательств.

Соответствие – является качественным измерителем аудиторских доказательств.

Подтверждением того, что аудиторские процедуры действительно были проведены, доказательства собраны, и могут быть проверены в любой момент времени является рабочая документация, оформленная надлежащим образом.

Это значит, что информация, содержащаяся в рабочих документах, должна быть обладать следующими характеристиками:

- полнота
- уместность
- надежность
- понятность

Рабочая документация составляется так, чтобы другой аудитор мог прийти к такому же выводу, как и аудитор их составивший.

Формирование списка недостатков по результатам аудита и аудиторского отчета [8]. После выполнения аудиторских процедур аудитор формирует список выявленных недостатков, которые впоследствии будут использоваться при формировании отчета по результатам аудита

Все выявленные недостатки должны базироваться на 4-х условиях (атрибутах). Критерии. Это стандарты, меры или ожидания, которые могут быть использованы в качестве оценки (того, что должно быть).

Пример: в отношении комплаенс целей – конкретное требование законодательства – персональные данные в информационной системе должны быть обезличены.

В отношении операционных целей - стандартом может являться как стандарт организации так и «лучшая практика» (например, как организовать процесс и контроли; COBIT, FERMA, ISO, информация из внешних источников, COSO и т.д.), конкретный целевой показатель (микро-уровень) - кол-во обрабатываемых операций или обслуживаемых клиентов и т.д. Важно:

понимание аудитором целей конкретного процесса, его построения и контролей, критериев и показателей достижения успеха, понимания специфических показателей (эффективности, продуктивности, рентабельности и т.д.), чтобы определить «идеальное», «стандартное» состояние. Здесь особенно важен профессионализм аудитора.

В отношении целей отчетности - соответствие критериям (полнота, своевременность, достоверность и т.д.), ИТ-контроли должны быть адекватными, чтобы обеспечить предотвращение и выявление значительных ошибок, отклонений от стандартов и других событий, в результат вводящих в заблуждение пользователей отчетности.

Условие. Это основанная на фактах информация, которую обнаружил аудитор в ходе выполнения задания (то, что есть на самом деле).

Например, аудитор провел процедуру тестирования операций по переводам Блиц за период с 01. по 25.03. 11г. и обнаружил переводы (из 50 - 25 переводов от 500 ; до 8 000 $), поступившие в адрес клиентов Банка, но не полученные ими в течение установленного срока, при этом сроки получения переводов истекли (от 5 до 20 дней), а работа по возврату средств отправителю, как это предусмотрено стандартом обслуживания не проведена.

Причина. Это объяснение существования различия между тем, что на самом деле есть и тем, что должно быть (т.е. объяснение, почему такое различие имеет место).

Например, предусмотренная процедурами банка ежедневная сверка сроков нахождения не полученных клиентами переводов не проводится. Кроме того, не предусмотрены процедуры автоматизированной обработки данных и уведомления о переводах с истекшим сроком получения, что позволило оптимизировать контрольную деятельность и своевременно сигнализировать о необходимости урегулирования таких ситуаций [22].

Следствие. Это риск, с которым сталкивается компания в результате существования различия между фактическим положением дел и тем, каким оно должно быть (влияние данного различия).

Например, как следствие, банк подвержен риску применения штрафных санкций за раскрытие персональных данных клиента.

Недостатки ранжируются по степени критичности.

При ранжировании недостатков можно использовать подход, указанный в таблице 2:

Таблица 2 – Ранжирование недостатков по степени критичности

Рейтинг недостатка	Определение	Уровень внимания
«1» – критический	Выявлены серьезные недостатки и уязвимости, выявлена неэффективность ИТ-контролей, наличие признаков мошенничества или имеют место серьезные инциденты.	Необходимы немедленные действия руководства для устранения недостатков
«2» –	Имеется ряд недостатков среднего уровня. ИТ-контроли частично эффективны. Имеют место инциденты средней степени.	Необходимо пристальное внимание руководства для минимизации недостатков в среднесрочной перспективе.
«3» – низкий	Отсутствуют недостатки/имеются недостатки низкого уровня. ИТ-контроли эффективны. Имеют место отельные области для улучшения	Рекомендуется внедрение отдельных улучшений в долгосрочной перспективе.

Аудиторский отчет является конечным продуктом деятельности аудита информационных технологий.

Содержание отчета должно быть четко сформулировано и понятно заинтересованным сторонам. Аудиторские отчеты являются основой для оценки работы внутреннего аудитора [9].

Основными задачами аудиторского отчета является:

- Обеспечение обоснованного, аргументированного информирования и предоставить гарантии (в отношении аудируемой области) менеджменту о результатах аудита
- Обеспечение операционного менеджмента/собственников процесса информацией о результатах оценки аудируемой области и необходимости корректирующих действий, направленных на улучшение процесса/деятельности
- Обеспечение аудиторов отчетностью для последующего отслеживания действий по результатам аудита

Передаваемая информация должна включать:

- Характеристики объекта аудита
- Выявленные недостатки
- Риски, к которым могут привести/к реализации которых привели выявленные недостатки
- Рекомендации по устранению/недопущению недостатков.

Отчет также может содержать краткие сведения общего характера (например, характер задания (плановый или по запросу), информация об организационной структуре клиента, видах и направлениях деятельности, которые являются объектом задания, а также соответствующие пояснительные замечания, рекомендации прошлых аудиторских заданий).

Аудитор обязан сформулировать цель аудиторского задания и, при необходимости, ожидаемые результаты от проведения данного задания (снижение издержек, повышение эффективности конкретного направления деятельности, определение способов мошенничества и защиты от них.)

Мониторинг исполнения мероприятий по результатам аудита. Как уже говорилось – все риски отчета считаются закрытыми, когда исполнены все мероприятия по устранению/недопущению недостатков [16].

План мероприятий по результатам аудита представляет собой список мероприятий по устранению/недопущению недостатков. Данный список содержит наименование о описание мероприятий, срок исполнения,

ответственных за исполнение. Аудитор осуществляет контроль за исполнением плана, путем анализа доказательств, подтверждающих его исполнение.

Схематически цикл внутреннего ИТ-аудита обозначен на рисунке 17.

Рисунок 17 – Цикл внутреннего ИТ-аудита

Аудиторская выборка. Одним из инструментов который использует аудитор в своей работе является аудиторская выборка. Применение выборки, позволяет сократить издержки на проведение аудита и обеспечивает приемлемые результаты в отношении точности и надежности получаемых аудиторских доказательств [16].

При проведении аудита применяются два типа тестирования - проверки на соответствие и проверки, по существу. Проверки на соответствие нацелены на оценку соблюдения принятого порядка оформления документов и соблюдения процедур. Проверка, по существу, позволяет контролировать

правильность стоимостных и других количественных показателей документов, операций и т.п.

Для проведения тестирования, тестируемая совокупность должна охватывать все единицы наблюдения, которые связаны с целью проверки и в одинаковой степени доступны для аудитора.

По целям и условиям проведения выборочные обследования можно разделить на два вида – нерепрезентативные и репрезентативные [21]. Для проведения выборки в зависимости от ситуации, могут использоваться оба вида.

Нерепрезентативная выборка заключается в отборе некоторой части единиц наблюдения из всей исследуемой совокупности. Нерепрезентативный отбор обычно производится на основе субъективных суждений аудитора.

Основанием для отбора может служить:

- Интуиция или «чутьё» аудитора в отношении «подозрительности» документов или их источников, опыт прошлых проверок, дополнительная информация от внешних сторон и т.п.
- Предположение аудитора о том, что отобранные единицы наблюдения наиболее характерны для проверяемой совокупности.
- Ориентированность аудитора на проверке наиболее крупных по стоимости документов.
- В случае, если проверяемая совокупность является не большой (менее 400 элементов), аудитор может провести нерепрезентативный отбор, при этом необходимо отбирать не менее 10% от общего количества элементов или их общей стоимости.

Целью репрезентативного выборочного исследования является получение характеристик генеральной совокупности по выборочным данным [17]. Полученная в ходе выборочного тестирования информация может быть распространена без больших погрешностей на всю проверяемую совокупность. Такую выборку называют репрезентативной в случае, если она получена специальными методами при соблюдении определенных условий,

основным из которых является равная вероятность для каждой единицы наблюдения совокупности попасть в выборку.

Репрезентативная выборка может быть следующих видов, различающихся по целям и соответственно по способам формирования выборок и методикам анализа:

- Атрибутивные выборки (Проверка на соответствие), используются при проведении проверок типа комплаенс или других специфических проверках.
- Выборка по стоимостным характеристикам совокупности (Проверка по существу), используется при проверках финансовой отчетности.
- Для проведения атрибутивной выборки аудитору необходимо:
- Сформулировать цель тестирования. Цель тестирования должна быть краткой и отражать результат, который аудитор намерен получить после проведения тестирования.
- Определить единицу наблюдения. Единицей наблюдения может быть документ, операция, событие и т.д., содержащий интересующий аудитора атрибут.
- Установить рамки исследуемой совокупности, причем каждая единица наблюдения (документ совокупности) должна быть одинаково доступна для отбора. Например, количество приходных кассовых ордеров за 20xx год, количество паспортов сделок, открытых в Филиале г. Алматы и т.д.
- Четко определить, какое свойство является тестируемым атрибутом; атрибут может быть единичным или комплексным (документ содержит набор реквизитов) и случай, когда отсутствует даже одно свойство или реквизит, документ рассматривается как отклонение. Например, наличие подписей, соответствие реквизитов.
- Принять уровень доверительной вероятности (F). По умолчанию уровень вероятности принимается равным 95%.
- Определить приемлемый верхний уровень точности оценки количества отклонений в совокупности (Т). По умолчанию уровень приемлемый

верхний уровень точности оценки количества отклонений в совокупности принимается равным 5%.

- Определить ожидаемую вероятность отклонения в выборке(p). По умолчанию ожидаемая вероятность отклонения в выборке составляет 3-7%, определяется на основе суждения аудитора об имеющихся контролях.
- Определить объем выборки(n). Объем выборки определяется аудитором на основании таблиц «Необходимых объемов выборки», после чего производится корректировка на конечный объем совокупности.
- Извлечь выборку из совокупности. Выборка извлекается автоматически на основе таблицы случайных чисел.
- Тестировать единицы наблюдения, оказавшиеся в выборке.
- Определить по выборке верхний уровень точности оценки количества отклонений(U). Верхний уровень точности оценки количества отклонений определяется аудитором на основании таблиц «Верхнего предела точности для совокупности», после чего производится корректировка на конечный объем совокупности.
- Принять решение о качестве тестируемой системы. Для принятия решения о качестве тестируемой системы аудитору необходимо сопоставить приемлемый верхний уровень точности оценки количества отклонений в совокупности (T) и верхний уровень точности оценки количества отклонений(U). В случае если U<=T, то у аудитора есть основания считать, что проверяемая система функционирует нормально. Если U>T, то аудитору необходимо увеличить объем выборки для получения дополнительной уверенности, если после этого неравенство не изменилось, то аудитору следует признать, что система функционирует ненадлежащим образом.

Для проведения выборки, по существу, аудитору необходимо:

- Сформулировать цель тестирования. Цель тестирования должна быть краткой и отражать результат, который аудитор намерен получить после проведения тестирования.

- Установить рамки исследуемой совокупности, причем каждая единица наблюдения (документ совокупности) должна быть одинаково доступна для отбора. Например, счета-фактуры, полученные за 201X год.
- Определить элементы с наибольшей стоимостью и ключевые элементы. Элементы с наибольшей стоимостью и ключевые элементы не включаются в выборку и проверяются обособленно сплошным методом.

К элементам с наибольшей стоимостью относятся элементы, значение которых превышает степень точности.

К ключевым элементам относятся такие элементы, которые с большой вероятностью содержат отклонения. Принять уровень аудиторского риска (AR). По умолчанию принимается равным 95%. Определить уровень существенности. Уровень существенности – предельное значение ошибки в статье отчетности, начиная с которой пользователи могут принимать неправильные решения или делать неправильные выводы. Определяется в пределах 3-7% от статьи отчетности [18].

Определить коэффициент совокупности (КС). Коэффициент совокупности определяется по формуле:

$$КС = \frac{(ОСД - НБ - КЛ)}{СТ}$$

где: ОСД- денежное выражение общего объема совокупности

НБ- суммарное денежное значение элементов с наибольшей стоимостью

КЛ- суммарное денежное значение ключевых элементов

СТ- степень точности (определяется как 75% от уровня существенности)

Значение коэффициента совокупности устанавливается в пределах от 10 до 35. В случае если значение КС меньше 10, то принимается за 10, если больше 35, то принимается 35.

Определить коэффициент надежности (КН). Коэффициент надежности определяется по формуле:

$$КН = -Ln(1 - УН)$$

где: УН-уровень надежности рассчитывается по формуле:

$$УН = 1 - DR$$

$$DR = \frac{AR}{IR * CR}$$

где: DR- риск необнаружения

AR- аудиторский риск (принимается на уровне 95%)

IR-неотъемлемый риск

CR- риск системы внутреннего контроля

Определить объем выборки (ОВ). Объем выборки определяется по формуле:

ОВ=КН*КС

где: КН- коэффициент надежности

КС- коэффициент совокупности

Определить интервал выборки (Ив). Интервал выборки определяется по формуле:

$$Ив = \frac{(ОСД - НБ - КВ)}{ОВ}$$

Определить начальную точку (НТ). Начальная точка определяется по формуле:

$$НТ = Ив * СЛЧИС$$

Осуществить выборку. Выборка осуществляется с помощью расчета кумулятивных сумм из совокупности документов и их сравнения с расчетными суммами. В выборку попадают единицы, на которые приходится кумулятивная сумма, равная или превышающая расчетные суммы [19].

Провести анализ полученных результатов и распространить ошибку на проверяемую совокупность. Распространение проверяемой совокупности осуществляется по следующей формуле:

$$Оп = Оф * \frac{(ОСД - НБ - КЛ)}{Сэв} + Онб + Окл$$

где: Оп – предполагаемая величина ошибки

Оф- фактическая величина ошибки, выявленная аудитором при проверке

Сэв – суммарная стоимость элементов выборки, проверенных аудитором

Онб- найденные аудитором ошибки при проверке элементов с наибольшей стоимостью.

Окл- найденные аудитором ошибки при проверке ключевых элементов.

Сопоставить предполагаемую величину ошибки с уровнем существенности. В случае если предполагаемая ошибка меньше или равна уровню существенности, то у аудитора есть основания полагать, что проверяемая статья является достоверной. Если предполагаемая ошибка больше уровня существенности, то аудитору следует признать, что проверяемая статья является не достоверной.

Рассмотрим примеры применения методов аудита информационных технологий при выполнении аудиторских заданий.

ПРИМЕР 1:

В Компании имеется критичная информационная ERP система, состоящая из ряда модулей (финансы, закупки, продажи, кадровый учет).

Аудитору необходимо провести аудит эффективности функционирования и безопасности указанной системы. Он выполняет следующий алгоритм шагов.

Собирает всю необходимую информацию о системе - технические требования к внедрению, функционал системы, регламент предоставления доступа, документацию подтверждающую легитимность использования систем (лицензии, договоры) [20].

- Запрашивает архитектуру системы
- Проводит интервью с владельцами системы
- Провести интервью, с лицами, осуществляющими поддержку систем

Идентифицирует и оценивает ключевые риски системы, такие как: невозможность интеграции с другими системами, остановка в обслуживании системы со стороны вендора (например, вендор перестает предоставлять обновления, что в свою очередь может привести к уязвимости системы), внешняя и внутренняя утечка информации, уничтожение и изменение информации, уничтожение данных журналов событий, встраивание скрытых алгоритмов в логику системы, сбои системы.

Идентифицирует ключевые ИТ- контроли, такие как: авторизация, аутентификация, разделение полномочий, ограничение доступа, преформатирование, резервное копирование, DPL-система, антивирус

Формирует программу аудита с необходимыми аудиторскими процедурами, такими как: инспектирование журналов событий, анализ матриц ролей и полномочий, интервью с представителями службы информационной безопасности, и т.д.

Осуществляет аудиторскую выборку, отбирая элементы в отношении которых будут проводиться аудиторские процедуры из имеющейся совокупности.

Выполняет процедуры, указанные в программе, и фиксирует

выявленные недостатки.

Готовит проект отчета по выявленным недостаткам и согласовывает его с аудируемыми.

Выпускает финальную версию отчета

Осуществляет мониторинг плана исполнения мероприятий по результатам аудита.

ПРИМЕР 2

Аудитор проводит аудит процесса управления непрерывностью предоставления сервисов ИТ (непрерывностью бизнеса).

Учитывая взаимозависимость современного бизнеса от ИТ-технологий - непрерывность бизнеса представляет собой способность организации к восстановлению критичных для ее деятельности ИТ-процессов в течение заданного периода времени. В ходе планирования деятельности многие компании по всему миру оценивают эффективность планов обеспечения непрерывности бизнеса и аварийного восстановления. В свою очередь, ИТ-аудиторы проводят оценку эффективности этих планов. План обеспечения непрерывности бизнеса представляет собой документ, в котором описывается, как организация предполагает функционировать вовремя и после возникновения кризисной ситуации. Он позволяет восстановить ИТ-процессы компании так скоро, как это необходимо для продолжения бизнеса.

Зависимость бизнеса от процессов ИТ очень ярко показала пандемия COVID-19 – глобальная пандемия коронавирусной инфекции, вызванная вирусом SARS-CoV-2. Первая вспышка была зафиксирована в Ухане, Китай, в декабре 2019 года. 30 января 2020 года Всемирная организация здравоохранения объявила эту вспышку чрезвычайной ситуацией, имеющей международное значение, а 11 марта — пандемией. По состоянию на 4 августа 2020 года в ходе пандемии было зарегистрировано свыше 18,2 млн случаев заболевания в более в чем 188 странах и территориях; свыше 693 тысячи человек скончались.

В условиях перевода персонала на удаленную работу способность к выживанию показали те организации, которые смогли:

- Своевременно обеспечить персонал оборудованием для удаленной работы или информацией, каким образом необходимо подключиться к удаленному рабочему столу;
- Обеспечить возможность вышеупомянутого подключения;
- Развернуть дополнительные мощности серверов и инфраструктуры;
- Обеспечить информационную защиту передаваемых данных (в том числе с помощью vpn-соединения);
- Обеспечить непрерывную поддержку пользователей.

Определим какие предпосылки необходимо проверить аудитору для того, чтобы сформировать программу аудита:

Аудитору необходимо убедиться в том, что:

- Компанией были определены критичные данные и критичные ИТ-системы подлежащие восстановлению в первую очередь;
- Компания провела идентификацию и оценку рисков, относящихся к непрерывности ИТ-процессов;
- Выполнен анализ воздействия на бизнес (Business impact analysis – BIA), включающий в себя: - анализ влияния потенциальных негативных событий на ключевые бизнес-процессы; - определение периода влияния негативных событий, превышение которого является недопустимым; - приоритетные сроки восстановления ключевых бизнес-процессов;
- Разработан план обеспечения непрерывности бизнеса, при разработке которого учитывались тип бизнеса, размер организации, ее структура и возможности;
- План обеспечения непрерывности бизнеса доведен до всех ответственных лиц;
- План обновляется на регулярной основе;
- Информация об актуализации плана также доводится до ответственных лиц;

- Проводится обучение сотрудников компании с целью ознакомления с планом;
- Проводится тестирование плана;
- В компании разработаны регламенты по работе с критическими информационными системами, включающие в себя информацию о процессе восстановления систем в случае сбоев, а также максимальном времени восстановления;
- Система резервного копирования компании позволяет восстанавливать критичные данные в необходимом объеме и установленный срок;
- Имеющиеся мощности являются достаточными для удаленной нагрузки на сеть большого количества пользователей;
- Налажена техническая поддержка пользователей;
- Заявки пользователей обслуживаются по степени критичности Определены критерии информационной безопасности в случае удаленного доступа пользователей к рабочим ресурсам со своего оборудования (требования к антивирусам, допустимое ПО и т.д.);
- Имеются резервные помещения/оборудование позволяющие (в случае недоступности основных помещений/оборудования) возобновить работу критичных подразделений;
- В компании имеется план реагирования на ИТ-инциденты;
- Данный план содержит результаты влияния на бизнес в случае сбоя или остановки критичных ИТ-систем, в том числе – допустимое время простоя и период, за который должна быть восстановлена информация;
- Данный план описывает меры, которые следует принять для восстановления бизнеса в нормальное русло, а также ресурсы необходимые для этого (кластеры, соглашения о взаимопомощи, практика «холодных» и «горячих» сайтов);
- Персонал, отвечающий за выполнение плана, осведомлен о своих обязанностях;
- План тестируется на регулярной основе.

Следовательно, в программу аудита попадут следующие процедуры:

- Инспектирование документации
- Проведение интервью с персоналом
- Запрос информации и документации
- Наблюдение (например, за проведением учений персонала по развертыванию критичного оборудования и критичных информационных систем).

Планирование

На этапе планирования задания аудитор должен достичь понимания объекта аудита. Это этап сбора информации об объекте аудита (в данном случае – ИТ-процессе) путем:

- Изучения регламентов и нормативно-правовых актов, регулирующих процесс;
- Интервью с владельцами процесса;
- Определения ключевых рисков, которым подвержен процесс;
- Определения ключевых контролей, позволяющих минимизировать указанные риски;
- Составлением программы аудита, с детальным описанием шагов и тестов, которые необходимо выполнить;
- Распределением обязанностей между членами аудиторской группы.

Выполнение («работа в поле»). Данный блок является непосредственно самим проведением аудита. Аудитор выполняет шаги из программы, разработанной в предыдущем блоке. Особое внимание уделяется тестированию ИТ-контролей (как общих, так и прикладных).

Коммуникация. Результатом тестирования является аудиторский отчет с описанием, выявленным недостатков (уязвимостей, слабости контролей, человеческих ошибок и случаев мошенничества). Указанный отчет доводится до высшего руководства компании и руководства объекта аудита (менеджмента, к чьей зоне ответственности относится проверяемый процесс).

Руководство объекта аудита, в свою очередь, разрабатывает план корректирующих мероприятий, позволяющих исправить недостатки, указанные в отчете, со сроками исполнения.

Но и на этом работа внутреннего аудитора не заканчивается. Он держит ситуацию на контроле, до полного исполнения корректирующих мероприятий, пока не будут закрыты все риски, указанные в аудиторском отчете.

1.3. Анализ шагов необходимых для повышения эффективности аудита информационных технологий

При анализе шагов для повышения эффективности аудита информационных технологий необходимо было проанализировать следующее:

- Штатная численной подразделения аудита информационных технологий
- Наличие регламентов, регулирующих область аудита информационных технологий
- Автоматизация работы подразделения аудита информационных технологий.

В ходе анализа штатной численности аудиторов было выявлено, что штатная численность аудиторов подразделения внутреннего аудита является оптимальной. Подразделение состоит из одного руководителя, обладателя сертификации CISA, трех ведущих аудиторов, а также двух старших аудиторов. В сравнении – в соответствии с Исследованием текущего состояния и тенденций развития внутреннего аудита финансовых организаций в России за 2020 год, проведенным Ассоциацией «Институт внутренних аудиторов» 62% опрошенных заявили, что в подразделениях внутреннего аудита нет специально выделенных ИТ-аудиторов.

В Компании имеются следующие регламенты по проведению аудитов информационных технологий:

- Положение о подразделении аудита информационных технологий;
- Методология проведения аудита информационных технологий (основана на Cobit 4.1 и, следовательно, являющаяся устаревшей)
- Инструкция о использовании программного обеспечения Primavera при проведении аудитов. Данное программное обеспечение законсервировано, и не используется несколько лет.

Автоматизация работы внутренних аудиторов не предусмотрена. Вся документация ведется в формате MS Office (Word, Excel, Power Point, и т.д.)

Модель внутреннего аудита (являющаяся основой для годового планирования), разрабатывается в формате MS Excel.

Отсутствует возможность удаленного управления ресурсами подразделения – контроль за рабочей документацией, постановка задач в трекере, с последующим отслеживанием статуса заданий, мониторинг исполнения мероприятий по итогам аудитов.

Отсутствует интеграция деятельности внутренних аудиторов с иными поставщиками гарантий.

В частности, в Компании имеются следующие подразделения второй линии защиты:

- Служба информационной безопасности;
- Департамент управления рисками;
- Департамент внутреннего контроля;
- Служба комплаенс.

Информация, подготавливаемая подразделениями второй линии защиты (в том числе информация об идентификации и оценке рисков, ИТ-контролях, выявленных инцидентах и проведенных расследованиях) не интегрирована в общую информационную базу, что затрудняет ее получение, а также не позволяет видеть целостную картину в отношении рисков и контролей Компании, для использования ее при планировании и проведении аудитов.

Таким образом, для повышения эффективности деятельности подразделения аудита информационных технологий Компании необходимо

внедрение решения по автоматизации работы внутренних аудиторов, в том числе интеграции работы аудиторов с подразделениями второй линии защиты.

В качестве инструмента автоматизации и интеграции предлагается рассмотреть работу GRC-системы (от английского Governance, Risk, Control – Корпоративное управление, Риски, Контроли), позволяющей упорядочить процессы внутреннего аудита информационных технологий, сократить объем времени на проведение аудитов, осуществлять обмен информацией в режиме реального времени, планировать ресурсы для проведения аудитов, способствовать накоплению знаний и их обмену с заинтересованными сторонами.

2. Методология решения поставленных вопросов

2.1. Автоматизация как инструмент повышения эффективности методов ИТ-аудита

Информация является одним из ключевых активов организации. Поэтому эффективное функционирование информационных потоков является жизненно важным условием для выживания организации в современных условиях. Учитывая ситуацию с пандемией, в том числе зависимость от стабильной работы информационных систем в условиях удаленной работы, быстрота восстановления информационных систем, а также оперативная работа технической поддержки являются процессами первой приоритетности.

В данный момент, благодаря разработанному плану непрерывности деятельности, основные процессы организации функционируют эффективно. То есть организация оказалась готова к работе во время кризиса. Не последнюю роль здесь сыграли усилия подразделения ИТ.

В то же время имеется ряд областей для улучшения.

Для повышения эффективности проведения ИТ-аудитов необходимо следующее:

- Возможность обмена информацией о присущих ИТ-рисках и контрольных процедурах, позволяющих минимизировать указанные риски;
- Наличие хранилища данных по бизнес-процессам Компании, рискам и контрольным процедурам;
- Возможность формирования Вселенной аудита и годового плана аудита;
- Возможность стандартизации и унификации аудиторской документации;
- Возможность контроля деятельности аудиторов, находящихся удаленно (например, в командировке);
- Возможность расчета трудозатрат и выделения ресурсов (например, построение диаграммы Ганта);

- Возможность координации деятельности подразделений, представляющих собой вторую и третью линию защиты, в том числе по вопросам идентификации и оценки рисков/контрольных процедур, выявления уязвимостей, а также непрерывности бизнеса.

Все вышеизложенное позволяет осуществить внедрение системы класса GRC (рисунок 18). Концепция GRC-систем появилась более 15 лет назад, и с тех пор она непрерывно развивается. Она объединяет в себе три основных компонента деятельности организации:

G - корпоративное управление (governance)

R- управление рисками (risk)

C - внутренний контроль (control). В некоторых случаях под литерой C обозначают соответствие (compliance)

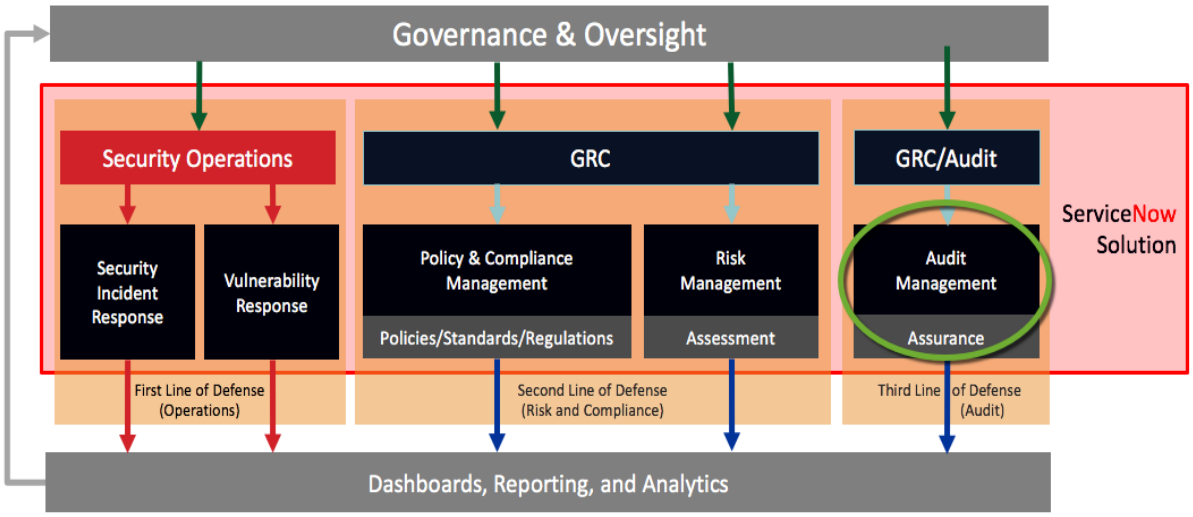


Рисунок 18 – Концепция GRC-системы

Концепция GRC-системы основана на интеграции информации, относящейся к корпоративному управлению, рискам и контролям, проактивном реагировании на возникающие инциденты, системности и риск-ориентированности.

Применительно к аудиту информационных технологий GRC-система позволяет использовать один из модулей называемый Audit Management (Управление аудитом).

Данный модуль позволяет:

- формировать модель ИТ-аудитов (с дальнейшей оценкой ИТ-процессов по риск-факторам)
- управлять всем жизненным циклом аудита, обеспечивая улучшенное стратегическое управление действиями, связанными с аудитом, а также интеграцию с функциями выявления рисков и контроля
- формировать годовой план аудита
- создавать отдельное аудиторское задание
- унифицировать формы рабочей документации аудитора
- управлять трудовыми ресурсами при проведении аудитов
- осуществлять идентификацию и оценку рисков
- вносить информацию о внутренних контролях
- осуществлять мониторинг корректирующих мероприятий
- осуществлять хранение базы знаний внутреннего аудита
- осуществлять аналитические процедуры при выполнении внутренних аудитов

Помимо данного модуля GRC-система может включать в себя следующие модули (рисунок 19):

Risk Management (Управление рисками) – модуль, позволяющий подразделению по управлению рисками проводить идентификацию, а также количественную и качественную оценку рисков. В том числе:

- Рисков информационной безопасности
- Рисков связанными с поставщиками ИТ-услуг/ИТ-систем
- Рисков, связанных с разработкой ИТ-систем

Модуль по управлению рисками можно адаптировать под любую из основных концепций управления рисками (COSO ERM, FERMA, ISO 31000 и т.д.)

Модуль позволяет проводить идентификацию и оценку рисков (в том числе рассчитывать количественные риски), осуществлять выбор мер реагирования выявление новых рисков. Business Continuity Management (Управление непрерывностью бизнеса) – позволяющий автоматизировать процессы оценки рисков непрерывности бизнеса, анализа влияния на бизнес (BIA), разрабатывать планы по восстановлению деятельности компании (рисунок 12). Система управления инцидентами (Security incident responce) позволяющая реагировать на возникающие инциденты в режиме реального времени. Система управления уязвимостями (Vulnerability responce) – позволяющая сканировать имеющиеся уязвимости в периметре информационной безопасности.

Рисунок 19 – Модули GRC-системы

Концепция GRC говорит о том, что компоненты аудита, рисков, контролей и непрерывности бизнеса тесно связаны между собой и находятся в постоянном взаимодействии. Концепция GRC подразумевает ведение

бизнеса, основанное на системности, проактивном и риск-ориентированном подходе. Это обеспечивает возможность получать необходимую и адекватную информацию в нужное время, позволяет ставить правильные цели и контролировать их достижение.

В целом GRC-система представляет собой интегрированный и целостный подход к организации корпоративного управления, управления рисками и внутреннего контроля, позволяющий убедиться в том, что компания действует соответствующим образом, в пределах своего риск-аппетита, и представляет собой взаимосвязь стратегии, процессов, технологий и человеческих ресурсов, повышая эффективность и результативность деятельности.

На российском и зарубежном рынках существует множество решений, позволяющих реализовать требуемый функционал.

Среди трудностей реализации следует отметить следующее:

- Высокую стоимость полноценного модуля GRC
- Отсутствие полноценной технической документации на русском языке (в случае приобретения зарубежного программного продукта)
- Сложность интеграции информации второй и третьей линии защиты
- Угрозу информационной безопасности (в случае если данные GRC-системы выводятся за периметр Компании – например, облачные решения)

Для осуществления выбора необходимой информационной системы Компании первым делом следовало оценить поставщиков аналогичного ПО.

Для этого необходимо разработать требования к информационной системе, которые могут включать:

- Ролевую модель доступа к данным ИС
- Поддержку удаленной работы с ИС
- Справочник бизнес-процессов, рисков и контролей
- Интуитивно-понятный интерфейс
- Возможность расчета трудозатрат и построения графиков
- Возможность отслеживания статуса выполняемых проектов

- Возможность интеграции с информационными системами Компании (системой электронного документооборота, системой бухгалтерского учета)
- Возможность одновременной работы нескольких пользователей
- Репутация поставщика
- Наличие технической документации
- Финансовое состояние поставщика
- Уровень цен
- Условия оплаты.

При определении требований можно использовать такой инструмент как квалификационная таблица с присвоением баллов (пример фрагмента таблицы указан на рисунке 20). Указанные требования позволяют выбрать ИТ-систему, наиболее оптимально удовлетворяющую требованиям Компании.

1.4. Разграничение прав доступа к системе					
Модель разграничения доступа	Ролевая модель разграничения доступа. Дискреционная модель разграничения доступа	Ролевая модель разграничения доступа	Ролевая модель разграничения доступа	Ролевая модель разграничения доступа. Системные роли: доступ к разделам системы на чтение или изменение, например: Администратор, Пользователь, Менеджер по управлению рисками и т.д. Специальные роли: доступ к отдельным элементам системы, например: Владелец актива, Администратор безопасности, Аудитор безопасности и т.д.	Ролевая модель разграничения доступа. Настраиваемые роли, на основании атрибутов объектов. Разграничение доступа ко всем объектам в системе с назначением прав на чтение, изменение, создание, выполнение групповых операций для конкретного пользователя/группы. Разрешения построены по принципу Модуль – Объект доступа – Право доступа – Политика

Рисунок 20 – Фрагмент квалификационной таблицы

2.2. Сравнительный анализ существующих методик и инструментов

Концепция полноценных GRC-систем (в том числе как инструментов для автоматизации методов внутреннего аудита) пришла на российский рынок сравнительно недавно.

Учитывая то, что данные системы позиционируются как системы для минимизации рисков, систематизации аудиторской деятельности, контроля за процессами компаний, одними из первых, кто обратил на них внимание были внутренние аудиторы (в том числе ИТ-аудиторы).

Огромную работу по популяризации использования данных систем проводит российский Институт внутренних аудиторов (ИВА). Тем использования автоматизации методов внутреннего аудита становится все более известной из опыта внедрения информационных систем рядом компаний.

GRC-системы внедряются как непосредственно самими вендорами, так и интеграторами (партнерами внедрения) выстраивающими информационные системы «под ключ», в соответствии с заданием клиентов.

Например, решение SAP GRC:

- В 2020 году компания «Норникель» завершила проект комплексной автоматизации внутреннего аудита на базе SAP Audit Management, являющегося одним из модулей SAP GRC. Партнером внедрения выступила компания PricewaterhouseCoopers. По информации полученной из пресс-релиза компании за счет использования единой системы компания повысила эффективность проведения аудиторских процедур и сократила сроки на подготовку аналитической отчетности.
- Другим примером может послужить внедрение модуля SAP GRC RM в компании Мегафон. SAP GRC RM представляет собой целостную систему управления рисками и внутреннего контроля бизнес-процессов, позволяющую реализовать полный цикл риск-менеджмента.

- К сожалению в российском секторе практически нет примеров, компании, которая бы смогла внедрить модуль SAP Process Control в котором автоматизированные средства контроля встраиваются в стандартные бизнес-процессы предприятия, что значительно сокращает необходимость проведения ручных проверок.

Компоненты решения SAP Access Control, SAP Risk Management SAP Process Control и SAP GRC Audit Management имеют возможность совместно использовать все данные и процессы, а также имеют удобные унифицированные интерфейсы и оптимизированы для различных областей и направлений бизнеса. Несмотря на это в связи с высокой стоимостью лицензий и сложностью внедрения на отечественном рынке не представлено компаний, которые могли бы продемонстрировать триединое интеграционное решение, позволяющее повысить эффективность работы внутренних аудиторов, риск-менеджеров и внутренних контролеров.

Решение RSA Archer. Модули RSA Archer – Audit Management, Business Continuity Management, Operational Risk Management стандартизируют и упрощают работу аудитора и риск-менеджера, сам процесс аудита и управления рисками, делая их эффективнее для всех «трех линий обороны» – бизнес-пользователей, риск-менеджеров и группы аудита. Модули RSA Archer позволяют автоматизировать полный аудиторский цикл, от построения Вселенной аудита до исполнения корректирующих мероприятий, осуществлять качественную и количественную оценку рисков, служить общей базой данных для подразделений второй и третьей линии защиты.

Данное решение является более популяризированным на западных рынках, но в настоящий момент завоевывает свою нишу и на российском рынке. В частности, в Росбанке используется платформа RSA Archer как единый инструмент для взаимодействия по большинству вопросов информационной безопасности.

Есть также ряд решений от иных вендоров. SAS Governance and Compliance Manager (от компании SAS) встроенные средства мониторинга и

коммуникации решения позволяют консолидировать мнения экспертов по рискам, специалистов службы внутреннего аудита и внутреннего контроля, а также руководителей бизнес-направлений, и использовать данную информацию для повышения эффективности процессов.

АВАКОР (Автоматизация внутреннего аудита, контроля и оценки рисков) от Компании Digital Design, являющееся одним из немногих российских решений имеющим функционал GRC-системы.

Имеются также программы исключительно для проведения внутреннего аудита, без включения интегрированной базы подразделений аудита, риск-менеджмента и иных подразделений чьим основным функционалом является минимизация рисков организации и выстраивание эффективной системы внутреннего контроля (примером является информационная система Team Mate).

Как мы видим, из результатов анализа – для повышения эффективности внутреннего ИТ-аудита, на рынке имеются не только одиночные решения по реализации методов годового планирования стандартизации аудиторского цикла, но и решения позволяющее аудиторам использовать единую базу знаний ряда подразделений компании отвечающих за риски и внутренний контроль, и осуществлять обмен этой информацией в режиме реального времени и координировать свои действия с указанными подразделениями с целью исключения дублирующих усилий.

3. Реализация функционала по проведению аудитов информационных технологий на базе GRC-системы

3.1. Предпосылки автоматизации функционала по проведению аудитов информационных технологий

Внедрение функционала по проведению аудитов информационных технологий на базе GRC-системы существенно повышает прозрачность и эффективность проведения аудитов на за счет использования единой базы данных, автоматизации аудиторских процедур, а также системы уведомлений и напоминаний, что позволяет сократить время выполнения рутинных процессов и исключить ошибки, связанные с ручной деятельностью.

Система позволяет охватить весь спектр процессов аудита информационных технологий:

- годовое планирование на макроуровне
- планирование отдельного аудиторского задания, в том числе ведение списка бизнес-процессов, рисков и ИТ-контролей
- подготовка программы аудита
- выполнение аудиторских процедур
- подготовка отчетности
- мониторинг исполнения мероприятий

Преимущества внедрения GRC-системы:

- Автоматизация «рутинных», типовых операций
- Обеспечение следования единым стандартам за счет унификации процедур
- Планирование ресурсов
- Использование шаблонов рабочей документации
- Доступность информации о выявленных рисках и реализовавшихся инцидентах
- Повышение исполнительской дисциплины бизнес-подразделений

- Отчетность и аналитика
- Организация с удаленной работы аудиторской команды

Основной задачей проекта является автоматизация деятельности Отдела аудита информационных технологий (далее - ОАИТ), обеспечению взаимодействия и обмена информацией между подразделениями второй и третьей линии защиты (департамента управления операционными рисками, департамента информационной безопасности, и т.д.), стандартизации и унификации аудиторской рабочей документации, повышению эффективности коммуникации с проверяемыми подразделениями, в том числе коммуникации по исполнению плана мероприятий.

В настоящее время в Компании выполнение функций аудита информационных технологий (стратегическое и годовое планирование, выполнение отдельных аудиторских заданий, мониторинг исполнения мероприятий) осуществляется посредством составления документации и предоставления отчетов в формате Word, Excel, Power Point, отсутствует возможность формировать необходимую аналитику в автоматическом режиме, отсутствует прямой доступ к данным подразделений второй линии защиты.

3.2. Функциональные требования к внедряемой системе

Для достижения поставленных перед внедряемой информационной системой целей, в системе должен быть реализован следующий функционал:

- Возможность ведения реестра основных бизнес-процессов Компании
- Возможность ведения реестра идентифицированных рисков
- Возможность оценки рисков с указанием вероятности и последствий риска, а также расчета его итогового значения.

  Формула для расчета итогового значения риска:

  ИТ_риск = В х П

  где,

В – вероятность возникновения риска

П - последствия возникновения риска

Возможность ведения реестра инцидентов, фиксируемых Департаментом информационной безопасности (DDOS-атаки, вредоносное ПО, утечка данных, сбои, и т.д.), с ранжированием инцидентов по степени критичности.

Возможность расчета итогового балла бизнес-процессов для определения их критичности на основе риск-факторов. Значения, параметры баллы и веса для риска- факторов используемых при оценке критичных процессов указаны в таблице 3:

Таблица 3 – Примеры риск-факторов

Риск-фактор	Баллы	Вес риск-фактора, %
Стоимость активов процесса	Менее 5 млн руб. От 5 до 500 млн руб. Более 500 млн руб.	20
Внимание к процессу	Внимание внутри Компании Внимание со стороны местной общественности Внимание со стороны глобальной общественности	20
Сложность процесса	Простые, рутинные операции Составные операции, вовлечение ряда сотрудников Сложносоставные операции, пересечение с другими процессами	15
Объем данных	Небольшой объем данных Средний объем данных Большой объем данных	20

Продолжение Таблицы 3

Риск-фактор	Баллы	Вес риск-фактора, %
Существенные изменения в процессе, персонале, ИТ-технологиях	Никаких существенных изменений за последние 12 месяцев Некоторые изменения в процессе, ключевом персонале процесса, информационных технологиях за последние 12 месяцев Существенные изменения в процессе, ключевом персонале процесса, информационных технологиях за последние 12 месяцев	15
Внимание менеджмента	Несущественное внимание Заинтересованность менеджмента в понимании ситуации по процессу Серьезная заинтересованность менеджмента в понимании ситуации по процессу	10

Вышеуказанная информация является базой для расчета итогового балла по каждому процессу. Процессы с наиболее высоким баллом (а соответственно более критические) автоматически попадают в план аудита на ближайший год.

Для расчета итогового балла используется следующая формула:

Итог_балл = $\sum$ (Б х В)

где,

Б – Балл

В – вес риск-фактора

Таблица 4 – Пример расчета итогового балла процесса «Управление изменениями

Риск-фактор	Баллы	Вес риск-фактора, %	Расчет	Итого
Стоимость активов процесса	2	20	2 х 0,2	0,4
Внимание к процессу	1	20	1 х 0,2	0,2
Сложность процесса	2	15	2 х 0,15	0,3
Объем данных	3	20	3 х 0,2	0,6
Существенные изменения в процессе, персонале, ИТ-технологиях	1	15	1 х 0,15	0,15
Внимание менеджмента	2	10	2 х 0,1	0,2
Итоговый балл процесса				1,85

По методологии ОАИТ – все процессы с итоговым баллом выше 1,5 считаются критическими. Следовательно, процесс «Управления изменениями» попадет в план аудита на ближайший год. Возможность формирования годового плана аудита на базе расчета риск-факторов бизнес-процессов. Возможность формировать отдельное аудиторское задание, состоящее из следующих блоков (рисунок 21).

Возможность загрузки/выгрузки рабочей документации (матрица рисков и контролей, программа аудита, отчетность) в/из системы.

Возможность формирования графика распределения трудовых ресурсов, а также учета фактически потраченного рабочего времени

Возможность формирования Плана мероприятий по результатам аудитов.

Возможность настройки простых формул расчета показателей.

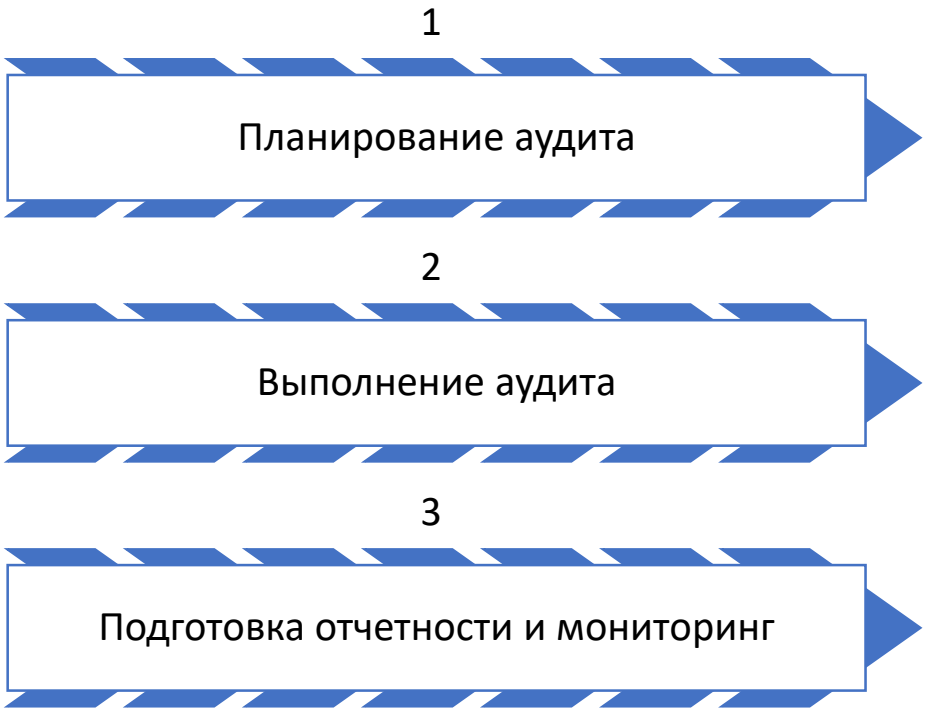


Рисунок 21 – Этапы аудита

Возможность формирования аналитических отчетов (количество выполненных аудитов в отношении к общему количеству аудитов, количество закрытых мероприятий по результатам проверок в отношении к общему количеству мероприятий, и т.д.).

3.3. Технические требования к внедряемой системе

Ролевая модель доступа к данным информационной системы. Предполагается ведение следующих ролей (таблица 4):

Таблица 5 – Ролевая модель

Роль	Функционал в ИС	Модуль
Директор ОАИТ	- Просмотр и редактирование списка бизнес-процессов Компании - Просмотр информации о рисках, контролях и инцидентах - Формирование Стратегического и Годового плана аудита - Назначение ролей пользователям системы - Просмотр и редактирование информации по всем текущим и завершенным аудитам - Просмотр и редактирование полного списка текущих/завершенных мероприятий по результатам проверок	GRC Audit Management
Руководитель проверки (назначается из числа аудиторов)	- Создание и редактирование отдельной аудиторской проверки - Назначение ответственных за области проверки в соответствии с программой проверки - Создание матрицы рисков и контролей - Создание программы проверки - Просмотр и утверждение рабочей документации по проверке - Просмотр и редактирование отчета по результатам проверки - Просмотр и редактирование текущих/завершенных мероприятий по результатам своих проверок	GRC Audit Management

Продолжение таблицы 5

Роль	Функционал в ИС	Модуль
Участник группы проверки (назначается из числа аудиторов)	- Просмотр и редактирование информации по своей области проверки - Просмотр и редактирование рабочей документации по проверке в рамках своей области проверки - Просмотр и редактирование отчета по результатам проверки	GRC Audit Management
Представитель Департамента управления рисками.	Актуализация информации по идентифицированным и оцененным рискам в модуль GRC Operational Risk-management	GRC Operational Risk-management
Представитель Департамента информационной безопасности	Актуализация информации по реализовавшимся ИТ-инцидентам	GRC Incident Management

Требования к интерфейсу системы.

Таблица 6 – Требования к интерфейсу

Язык интерфейса	Русский
Возможность удаленной работы	Да
Тип подключения	Толстый клиент WEB

Требования по миграции данных – отсутствуют

Требования к доступности и производительности системы.

Таблица 7 – Требования к доступности и производительности

Режим работы	24x7
RTO	72 часа
RPO	24 часа
Резервное копирование	Период хранения резервных копий: – 30 дней Период хранения журналов событий безопасности – 30 дней. По истечении 30 дней – журналы автоматически архивируются и хранятся на протяжении 1 года

Требования к конфигурации системы

Таблица 8 – Требования к конфигурации

Режим работы	24x7
RTO	72 часа
RPO	24 часа
Резервное копирование	Период хранения резервных копий: – 30 дней Период хранения журналов событий безопасности – 30 дней. По истечении 30 дней – журналы автоматически архивируются и хранятся на протяжении 1 года

Требования к конфигурации рабочих мест пользователей.

Таблица 9 – Требования к конфигурации рабочих мест пользователей

Параметр	Требование
CPU	ядра – не менее 4 частота – не менее 3.0 Ггц каналы памяти – 2 Intel Core i3, или выше.
ОЗУ	4 Гб и выше
HDD/SSD	500/200
Комплектация	Клавиатура, манипулятор-мышь, кабель питания
Системное ПО	ОС MS Windows 10 Pro

Требования к информационной безопасности системы. Система должна удовлетворять требованиям внутренних нормативных документов Компании по информационной безопасности. Система должна обеспечивать защиту от несанкционированного доступа, на основе ролевой модели. Срок хранения информации о событиях ИБ в журналах аудита Системы должен составлять – 90 дней. По истечении указанного срока, журналы архивируются и хранятся на протяжении 365 дней.

Требования к документации. При реализации проекта по внедрению информационной системы должна быть сформирована следующая документация.

- Протокол инвестиционного комитета
- Устав проекта
- Техническое задание
- Описание функционала системы
- Регламент предоставления доступа к системе
- Методика испытаний системы
- Приказ о вводе системы в промышленную эксплуатацию

Нефункциональные требования к информационной системе:

- Обеспечение целостности данных
- Обеспечение доступности данных
- Устойчивость системы к сбоям
- Масштабируемость системы при увеличении количества бизнес-пользователей
- Понятность и легкость использования системы, в том числе интуитивно понятный интерфейс

3.4. Особенности проверки исполнения плана мероприятий по результатам аудитов.

При проверке исполнения Плана мероприятий по результатам аудитов возникает следующие сложности:

- мероприятия растянуты во времени
- срок исполнения разных мероприятий не совпадает
- исполнителями по разным мероприятиям может быть достаточно широкий круг лиц – представителей различных подразделений.

Для решения данного вопроса в системе реализован следующий функционал. Система GRC интегрируется с почтовой системой MS Outlook с помощью сервиса Microsoft Exchange. В системе GRC настроен режим отправки исполнителям уведомлений, напоминающих о необходимости выполнения мероприятий. Отправка уведомлений происходит за 2 недели, за неделю и за 3 дня до наступления указанных мероприятий, а также в день являющийся крайним сроком для исполнения мероприятий. Система также позволяет осуществить выгрузку всех мероприятий в формат MS Excel. Неисполненные мероприятия срок исполнения, по которым уже наступил для повышения эффективности визуального восприятия автоматически выделяются красным цветом.

4. Тестирование разработанного подхода к процессу проведения внутреннего аудита информационных технологий и анализ результатов.

4.1 Модули GRC системы

Разработка и внедрение системы GRC проводилось в соответствии с техническим задание и функционально-техническими требованиями на основе коробочного решения, с определенными доработками, указанными заказчиком (Компанией).

Рассмотрим работу каждого из модулей внедряемой системы.

Модуль «Управление аудитом»:

Позволяет настраивать процесс проведения аудитов (рисунок 22) в соответствии со стандартами Международного института внутренних аудиторов (IIA), Международной ассоциации аудита информационных систем и контролей (ISACA).

Модуль позволяет:

- Вести иерархический список бизнес-процессов организации.
- Осуществлять формирование годового плана аудита на основе анализа риск-факторов, информации, получаемой из модуля управления рисками и модуля управления инцидентами.
- Назначать ответственных за проведение отдельного аудиторского задания.
- Контролировать ход задания.
- Осуществлять хранение рабочей документации.
- Ограничивать доступ к тем или иным подмодулям системы
- Обмениваться информацией с модулями по управлению рисками и управлению инцидентами на основе простой интеграции.
- Обмениваться информацией с MS Outlook посредством инструмента Microsoft exchange.

- Осуществлять мониторинг исполнения мероприятий по результатам аудитов.

Рисунок 22 – Процесс проведения аудитов»

Модуль по управлению рисками

Позволяет настраивать процесс управления рисками Компании в соответствии с лучшими мировыми стандартами управления рисками (COSO ERM, FERMA, ISO 31000)

В частности, в Компании было принято решение о настройке модуля в соответствии с методологией COSO (рисунок 23). Для этого в модуле предусмотрено формирование иерархического реестра рисков.

Рисунок 23 – Процесс управления рисками организации

Существует возможность «провалиться» в карточку любого из рисков и просмотреть следующую информацию:

- Описание риска
- Тип риска (стратегический, операционный, комплаенс, отчетности, ИТ)
- Вероятность риска (рассчитывается по 5-бальной шкале)
- Влияние риска (рассчитывается по 5-бальной шкале)
- Итоговое значение первоначального риска
- Выбор мер реагирования на риск (принятие, уклонение, перераспределение, снижение). Каждая из мер представляет собой конкретное мероприятие.
- Итоговое значение остаточного риска.

Указанные риски имеют реляционные связи со списком бизнес-процессов (каждому из процессов присущ тот или иной риск, или их совокупность.)

Существует возможность визуализации информации по рискам с помощью предварительно настроенных отчетов, панелей управления рисками.

Информация из модуля используется ИТ-аудиторами на этапе планирования аудита, при проведении идентификации и оценки рисков объекта аудита.

Модуль "Управление инцидентами ".

Автоматизирует процедуры регистрации, обработки инцидентов ИБ, оповещения о них, хранения статистики и результатов расследования инцидентов ИБ (рисунок 24).

Рисунок 24 – Процесс управления инцидентами

В частности, модуль фиксирует информацию о следующих инцидентах:

- Несанкционированное изменение конфиденциальной информации
- Несанкционированное удаление конфиденциальной информации
- Внедрение вредоносного ПО (вирусы, трояны, логические бомбы) на сервера Компании.

4.2. Тестирование работы модулей.

С целью тестирования функционала системы были выполнены следующие шаги.

В модуле «Управление аудитами» в информационную систему были внесены следующие бизнес-процессы:

- Управление инцидентами,
- Управление изменениями
- Управление конфигурациями
- Управление ИТ-проектами

Были внесены следующие риск-факторы:

- Стоимость активов процесса
- Внимание к процессу
- Сложность процесса
- Существенные изменения в процессе, персонале, ИТ-технологиях

Протестировано годовое планирование внутренних аудитов информационных технологий, на примере процесса «Управление ИТ-активами», а именно – проведена оценка тестируемого процесса по риск-факторам.

Подготовлена Программа аудита по процессу «Управление ИТ-активами», включающая распределение аудиторских процедур по следующим трем основным блокам:

- Планирование аудита
- Выполнение аудита
- Подготовка отчетности и последующий мониторинг исполнения мероприятий по результатам аудита.

В Программу аудита была добавлена информация о сроках исполнения аудиторских процедур и ответственных за исполнение.

В Модуле «Управление рисками» была создана карточка следующего риска - риск неэффективности внедрения ИТ-проекта.

В карточке каждого риска были заполнены следующие данные:

- Вероятность риска
- Последствия риска
- Тип риска
- Итоговое значение первоначального риска
- Мероприятия по минимизации риска

- Значение остаточного риска

Пример приведен в таблице 10.

Таблица 10 - Карточка риска неэффективности внедрения ИТ-проекта

Наименование	Риск неэффективности внедрения ИТ-проекта
Вероятность риска (1-5)	3
Последствия риска (1-5)	2
Итоговое значение первоначального риска	6
Мероприятия по минимизации риска	- Создание проектной команды - Разработка Устава проекта - Периодический контроль сроков исполнения проекта
Значение остаточного риска	4

В Модуле «Управление инцидентами» были заведены два следующих инцидента - риск утечки данных

Риск утечки данных.

- Внесение несанкционированных изменений в данные информационных систем
- Уничтожение данных в результате сбоя информационной системы

Информация из модуля «Управление рисками» и «Управление инцидентами» была перенесена в блок планирования аудиторской проверки управления ИТ-проектами модуля «Управление аудитами».

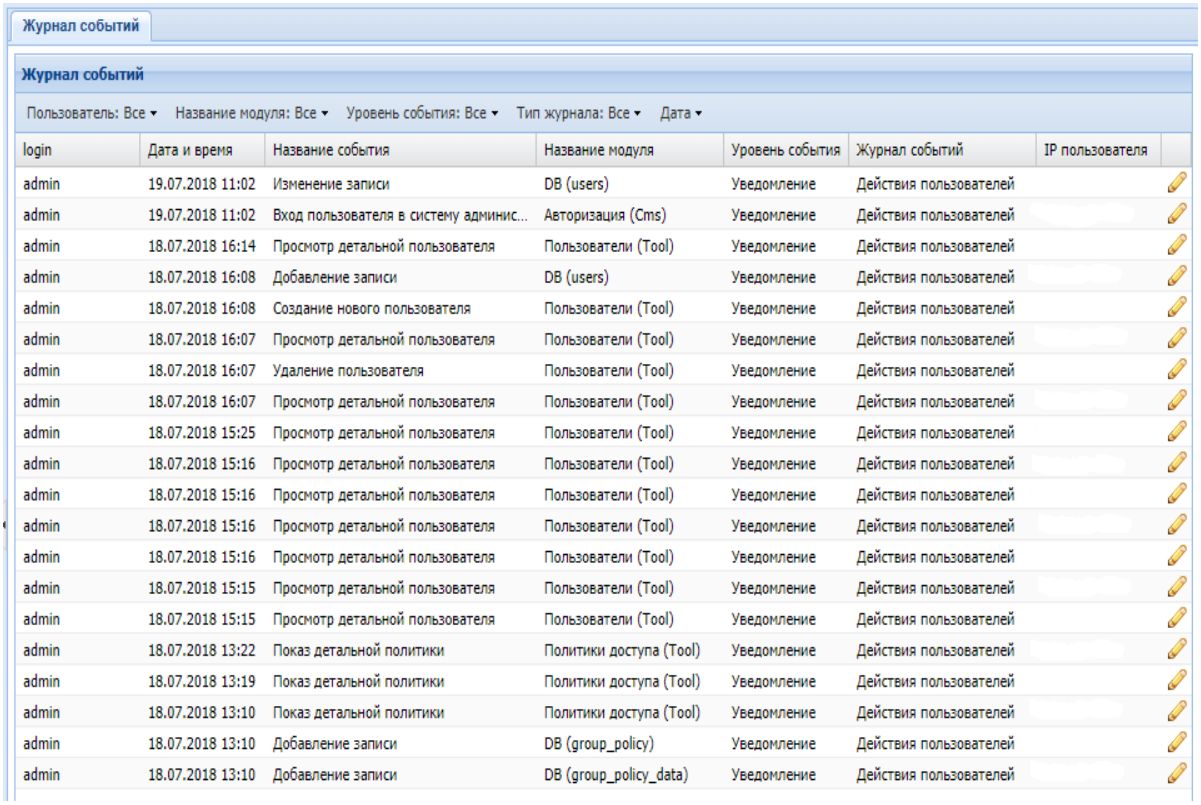
По результатам аудита в модуле «Управление аудитами» были зафиксированы результаты аудита, со следующими рекомендациями:

- Регламентировать процесс управления ИТ-проектами
- Внедрить специализированное программное обеспечение по управлению ИТ-проектами.
- Провести обучение ключевых сотрудников Департамента проектов дисциплине в области управления проектами – PMI.

Был создан план мероприятий по результатам аудита, назначены ответственные за его исполнение и сроки исполнения.

Была произведена отправка уведомления о наступлении срока исполнения мероприятия ответственному за исполнение.

Проведена проверка фиксации событий в журнале событий (рисунок 25). Результат – имеет место фиксация инициатора события, самого события, даты и времени события.



login	Дата и время	Название события	Название модуля	Уровень события	Журнал событий	IP пользователя
admin	19.07.2018 11:02	Изменение записи	DB (users)	Уведомление	Действия пользователей	
admin	19.07.2018 11:02	Вход пользователя в систему админис...	Авторизация (Cms)	Уведомление	Действия пользователей	
admin	18.07.2018 16:14	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 16:08	Добавление записи	DB (users)	Уведомление	Действия пользователей	
admin	18.07.2018 16:08	Создание нового пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 16:07	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 16:07	Удаление пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 16:07	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 15:25	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 15:16	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 15:16	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 15:16	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 15:16	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 15:15	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 15:15	Просмотр детальной пользователя	Пользователи (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 13:22	Показ детальной политики	Политики доступа (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 13:19	Показ детальной политики	Политики доступа (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 13:10	Показ детальной политики	Политики доступа (Tool)	Уведомление	Действия пользователей	
admin	18.07.2018 13:10	Добавление записи	DB (group_policy)	Уведомление	Действия пользователей	
admin	18.07.2018 13:10	Добавление записи	DB (group_policy_data)	Уведомление	Действия пользователей	

Рисунок 25 – Журнал событий

4.3. Особенности интеграции модулей GRC-системы.

Все три модуля GRC-системы тесно взаимосвязаны друг с другом и позволяют осуществить следующий обмен данными.

При аудите одного из бизнес-процессов имеется возможность проверить – были ли в прошлом идентифицированы риски, относящиеся к данному процессу и занести информацию о них в блок «Планирование» текущего аудита.

Имеется возможность проверить – были ли в прошлом идентифицированы инциденты информационной безопасности, относящиеся к данному процессу и занести информацию о них в блок «Планирование» текущего аудита.

В случае выявления новых рисков/реализовавшихся инцидентов в аудируемом бизнес-процессе – имеется возможность доведения указанной информации до соответствующих владельцев модулей «Управление рисками» и «Управление инцидентами».

В случае наступления срока исполнения мероприятия по результатам проверки – система GRC направляет напоминание о необходимости исполнения владельцу мероприятия посредством почтовой программы MS Outlook.

Ниже на схеме (рисунок 26) показана архитектура взаимодействия модулей GRC-системы.

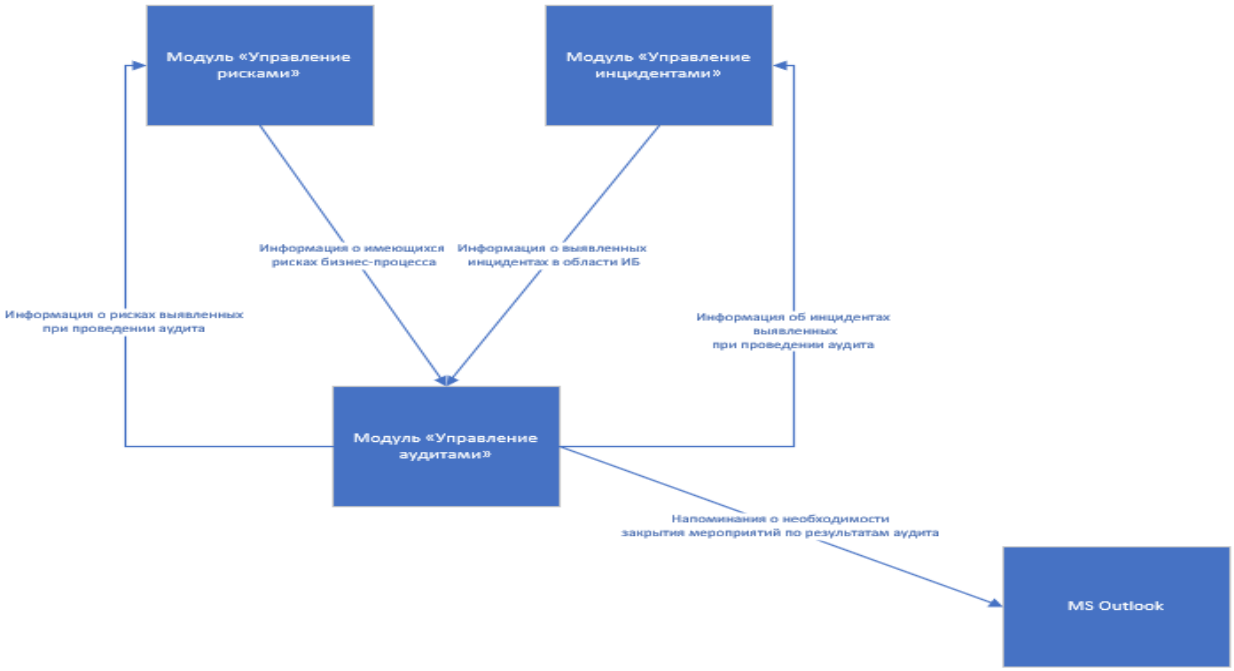


Рисунок 26 – Взаимодействие модулей GRC-системы

4.4. Оценка эффективности GRC-системы

С целью построения выводов по проекту, подведения его итогов, оценивается эффективность внедряемой GRC-системы.

Внедрение указанной системы позволяет:

- Выстраивать полный цикл аудитов информационных технологий, начиная от годового планирования и заканчивая мониторингом плана исполнения мероприятий по результатам аудитов (в том числе автоматизировать построение годового плана аудита).
- Использовать единую базу данных по рискам и реализовавшимся инцидентам.
- Применять единую терминологию и методологии по рискам
- Использовать актуальную информацию по рискам и инцидентам
- Использовать общий перечень бизнес-процессов Компании
- Осуществлять контроль за проведением аудитов на всех стадиях

– Снизить трудозатраты на проведение аудитов за счет исключения избыточной документации

По результатам тестирования GRC-системы можно сделать вывод об успешном выполнении всего необходимого функционала. Внедрение указанного функционала позволяет автоматизировать процессы аудита информационных технологий, снизить трудозатраты на проведение аудитов, стандартизировать работу аудиторов, а также поддерживать информационную связь с подразделениями второй линии защиты.

Заключение

В качестве объекта исследования выступает компания ООО «City Plus». Основными информационными системами Компании являются следующие:

- SAP – поддерживает модули по закупке и продажам, а также вопросы кадрового учета
- 1С: Предприятие (версия 8.2) – позволяет вести учет основных средств и заработной платы. Модуль кадрового учета системы SAP интегрирован с модулем по учету заработной платы 1С;
- СЭД Директум – система электронного документооборота Компании;
- Acronis Backup – система по управлению резервным копированием.

Основными целями проведения внутреннего аудита информационных технологий Компании являются

- оценка эффективности и результативности ИТ-процессов и систем
- оценка эффективности работы ИТ-специалистов
- оценка защищенности информационных активов Компании от внешних и внутренних угроз
- разработка рекомендаций по повышению эффективности работы Компании, ее конкурентного преимущества.

Для осуществления всего вышеизложенного необходима структуризация работы внутренних аудиторов, получение информации от подразделений второй линии защиты в оперативном режиме, автоматизация процесса годового планирования и т.д.

Одним из наиболее популярных решений на текущий момент является внедрение GRC-системы, позволяющей повысить прозрачность и эффективность проведения аудитов на за счет использования единой базы данных, автоматизации аудиторских процедур, а также системы уведомлений и напоминаний, что, в свою очередь позволяет сократить время выполнения рутинных процессов и исключить ошибки, связанные с ручной деятельностью.

По результатам тестирования GRC-системы можно сделать вывод об успешном выполнении всего необходимого функционала. Внедрение указанного функционала позволяет автоматизировать процессы аудита информационных технологий, снизить трудозатраты на проведение аудитов, стандартизировать работу аудиторов, а также поддерживать информационную связь с подразделениями второй линии защиты в части актуализации информации о выявленных рисках, контролях и произошедших инцидентах.

Список используемой литературы

1. Автоматизация процессов внутреннего аудита [Электронный ресурс] URL: https://www.audit-it.ru/articles/audit/a1011009/1026526.html (дата обращения: 18.04.2021).
2. Агабекян, О.В., Макарова, К.С. Аудиторское заключение: формы выражения мнения, составление и представление // Аудиторские ведомости. 2019. N 3. с. 13 — 19.
3. Внутренний аудитор № 3 (11), 2020 – 105 с.
4. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью. М.: Стандартинформ, 2006. — 56 с.
5. ГОСТ Р ИСО/МЭК 22301—2014 Системы менеджмента непрерывности бизнеса.// М. Стандартинформ., 2015. – 28 с.
6. ГОСТ Р ИСО/МЭК 27001-2005. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2006. — 31 с.
7. Елисеева И.И., Терехов А.А. Статистические методы в аудите. - М.: Финансы и статистика, 1998 с. 105
8. Казакова Н.А. Аудит для магистров по российским и международным стандартам: учебник / под ред. проф. Н.А. Казаковой. — М.: ИНФРА-М, 2017. — 345 с.
9. Крышкин О.Н. Настольная книга по внутреннему аудиту. Риски и бизнес-процессы. Учебник. — М.: Альпина Паблишер, 2018. — 478 с.
10. Национальный стандарт РФ ГОСТ Р ИСО 22301- 2014 «Системы менеджмента непрерывности бизнеса. Общие требования» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 17 октября 2014 г. N 1351-ст) - 28 с.

11. Национальный стандарт РФ ГОСТ Р ИСО 22313- 2015 «Менеджмент непрерывности бизнеса. Руководство по внедрению» (утв. приказом Федерального агентства по техническому регулированию и метрологии от 18 ноября 2015 г. N 1852-ст) – 48 с.

12. Остапенко О. А., Карпеев Д. О., Асеев В. Н. Риски систем: оценка и управление. М.: Горячая линия—Телеком, 2007. — 247 с

13. Палканов И.С., Рачков В.Е. Внутренний аудит информационной безопасности как инструмент получения объективных оценок состояния информационной безопасности организации // Студенческая наука для развития информационного общества. - 2019. - № 7. - с. 153-161

14. Роб Ингланд Овладевая ITIL. М.: Лайвбук, 2011. — 200 с.

15. Ситнов А.А., Уринцов А.Э. Аудит. Учебник информационных систем.— М.: Юнити-Дана, 2019. — 240 с.

16. Скобара, В.В. Аудит; методология и организация. — М.: «Дело и сервис», 2018. — 576 с.

17. Спиридонов Д.В. Современные методы оптимизации работы IT-подразделения [Электронный ресурс] URL: https://www.elibrary.ru/item.asp?id=35349144 (дата обращения: 24.04.2021).

18. Суворова, С.П. Основы внутрифирменной стандартизации аудиторской деятельности: учеб. пособ. / С.П. Суворова, Н.В. Парушина, Е.В. Галкина, А.М. Ковалева. - М.: ИД ФОРУМ, Инфра-М, 2011. - 336 с.

19. Суглобов А.Е. Аудит, Учебник для бакалавров. М: Кнорус, 2009 – 240 с.

20. Сучалкина Е.А. Роль аудита в системе экономической безопасности предприятия // Актуальные проблемы менеджмента, экономики и экономической безопасности. - 2020. - №8. - С. 228-231.

21. Терехов, А.А., Терехов, М.А. Контроль и аудит: основные методические приемы и технология. — М.: Финансы и статистика, 2019. — 208 с

22. Токун М. Линии защиты компании. Карта гарантий. [Электронный ресурс] URL: https://www.audit-it.ru/articles/audit/a104/979017.html (дата обращения: 18.05.2021).

23. Четыркин Е.М. Выборочные методы в аудите. М:Кнорус, 2010 – 132 с.

24. Чехлов М.Ю. Аудит обеспечения непрерывности бизнеса. . [Электронный ресурс] URL: https://kachestvo.pro/kachestvo-upravleniya/instrumenty-menedzhmenta/audit-obespecheniya-nepreryvnosti-biznesa/ (дата обращения 15.01.2021).

25. Шин С.А. Взаимосвязь информационной безопасности и внутреннего аудита компании: региональное исследование // Вестник Атырауского Университета имени Х.Досмухамедова. - 2019. - № 4. - С. 158-167.

26. COBIT 4.1 //ISACA. 2007 - 196 с.

27. COBIT 5 for Assurance//ISACA 2013 - 266 с.

28. ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements (Безопасность и устойчивость. Системы менеджмента непрерывности бизнеса. Требования) – 30 с.

29. Software Assurance Maturity Model. [Электронный ресурс] URL: https://www.opensamm.org/ (дата обращения 01.05.2021).

30. Weber Ron.EDP Auditing – Conceptual Foundations and Practise – UK/ Издательство «Mcgraw-Hill» 1988 – с.22