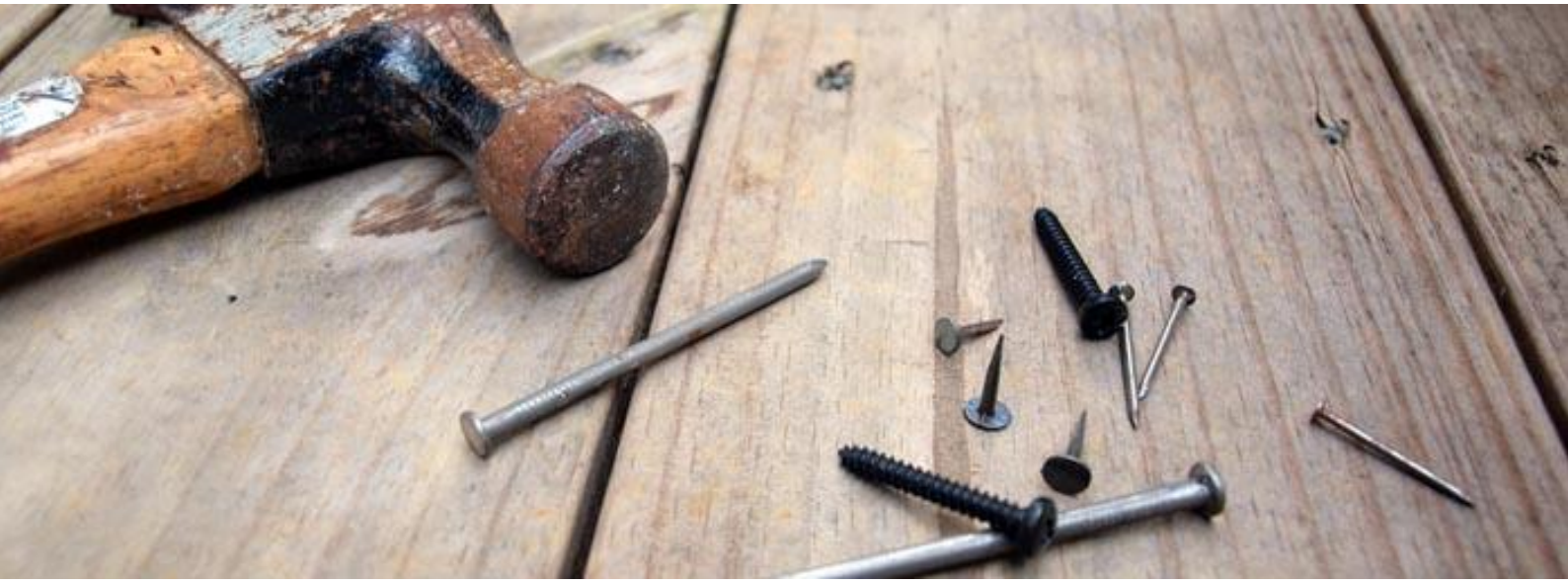
105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Как сделать проект по ISO 27001 и получить сертификат

Методические рекомендации



105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Содержание

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Введение

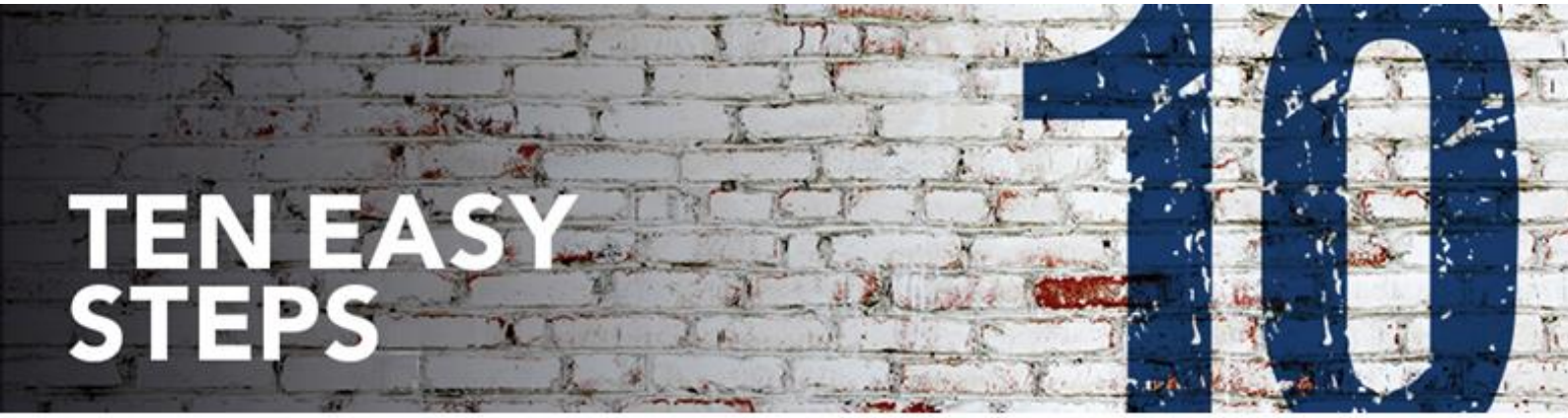
Это методическое пособие основано на реальном практическом опыте специалистов компании IT Task и содержит в себе основные правила, требования и рекомендации для построения и внедрения системы управления информационной безопасностью в соответствии с требованиями международного стандарта ISO/IEC 27001. Все примеры, материалы и подход в целом, приведенные в этом пособии, являются частью реальных проектов построения и последующей сертификации системы управления информационной безопасностью (далее – СУИБ) компаний.

Безусловным достоинством этого пособия мы считаем наличие в нем перечня основных документов, требуемых в процессе создания и подготовки системы, а также примеры заполнения этих документов.

Мы не стремились здесь придумать что-то новое в процессе построения и подготовки системы управления информационной безопасностью, но постарались передать свой практический опыт в этом вопросе.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

1. 10 шагов подготовки к сертификации по стандарту ISO/IEC 27001



В этом разделе мы изложили перечень основных шагов, которые нужно выполнить, чтобы создать систему управления информационной безопасностью и подготовить компанию к прохождению сертификационного аудита BSI.

Итак, **10 основных шагов к подготовке и сертификации СУИБ:**

1. Выбираем процесс(ы) (область деятельности), который(е) будем сертифицировать.
2. Собираем команду; если необходимо, то привлекаем специалистов.
3. Проводим внутренний аудит с целью определить текущее состояние СУИБ компании.
4. Проводим идентификацию ресурсов, которые входят в выбранную область деятельности.
5. Определяем ценность ресурсов.
6. Считаем риски.
7. Готовим пакет документов: политики, стандарты, положения, процедуры и т. п.
8. Внедряем политики, стандарты, положения, процедуры и т. п.
9. Проводим внутренний аудит и оценку СУИБ с учетом проведенной работы по внедрению организационных и технических мер.
10. Подаем заявку на проведение сертификационного аудита.

Далее вы найдете более детальную информацию по каждому из шагов: что и как. Но прежде давайте выясним, зачем нужен сертификат.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

2. Зачем нужен сертификат ISO/IEC 27001

Стандарт ISO 27001 определяет процессы, которые предоставляют бизнесу следующие возможности:

1) установление, применение, пересмотр, контроль и поддержание эффективной системы менеджмента информационной безопасности;
2) защита предприятия от неправильного обращения с файлами и документами и/или от кражи сотрудниками коммерческих тайн предприятия;
3) установление требований к разработке, внедрению, функционированию, мониторингу, анализу, поддержке и совершенствованию документированной системы информационной безопасности в контексте существующих бизнес-рисков организации.

Наличие сертифицированной системы менеджмента информационной безопасности и **сертификата** ISO/IEC 27001:2013 **позволяет** организации:

1) выявить слабые места системы менеджмента информационной безопасности и существующие угрозы информационной безопасности действующих бизнес-процессов;
2) определить возможные риски и принимать необходимые управленческие решения;

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

3) обеспечить эффективную защиту информации в критических ситуациях;
4) оптимизировать затраты, связанные с поддержкой системы безопасности;
5) повысить авторитет организации на отечественном рынке и открыть выход на зарубежные рынки;
6) улучшить отношения с органами надзора, упростить процедуру получения необходимых разрешительных документов.

Можно сказать, что **сертификация по стандарту ISO/IEC 27001** служит прямым подтверждением высокого качества предоставляемых услуг компании и позволяет обеспечить:

- ✓ конфиденциальность информации клиентов – гарантирует, что доступ к информации получают только те, кто уполномочен иметь доступ;
- ✓ целостность информации – обеспечивает точность и полноту информации и методов обработки;
- ✓ доступность информации – гарантирует авторизованным пользователям доступ к информации и сопутствующим ресурсам, когда это необходимо.

В таблице, представленной ниже, мы постарались отразить все выгоды от сертификации как для компании, заинтересованной в таком сертификате, так и для клиента этой компании.

Выгоды компании	**Выгоды заинтересованных сторон**
Способствует успешной реализации продукции (услуг): ✓ повышает качество и конкурентоспособность продукции; ✓ способствует росту удовлетворенности клиентов/потребителей; ✓ расширяет рыночные возможности; ✓ улучшает имидж фирмы в глазах общественности;	**Потребители** *получают услуги, которые:* ✓ соответствуют качественным требованиям; ✓ надежны; ✓ оказываются своевременно. **Сотрудники организации** *получают выгоды от:*

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

- ✓ повышает доверие со стороны партнеров и клиентов.

Повышает культуру менеджмента и уровень управляемости:

- ✓ улучшает оптимизацию управленческих процессов;
- ✓ большинство информационных активов становятся наиболее понятными для менеджмента компании;
- ✓ выявляются основные угрозы безопасности для существующих бизнес-процессов;
- ✓ рассчитываются риски и принимаются решения на основе бизнес-целей компании;
- ✓ обеспечивается эффективное управление системой в критических ситуациях;
- ✓ проводится процесс выполнения политики безопасности;
- ✓ четко определяется личная ответственность;
- ✓ управление компанией выводится на уровень мировой практики менеджмента.

Экономит затраты на разработку, производство и применение продукции (услуг):

- ✓ снижение и оптимизация стоимости поддержки системы безопасности;
- ✓ профилактика несоответствий и сбоев в работе;
- ✓ уменьшение количества ошибок.
- ✓ улучшения рабочих условий;
- ✓ большего удовлетворения работой;
- ✓ улучшения морального климата.

Собственники и инвесторы

получают выгоды от:

- ✓ роста конкурентоспособности компании на российских и международных рынках;
- ✓ повышения инвестиционной привлекательности компании;
- ✓ увеличения прибыли на вложенный капитал;
- ✓ увеличения доли рынка и улучшения результатов деятельности организации;
- ✓ повышения капитализации компании;
- ✓ увеличения шансов на победу в тендерах и конкурсах.

Партнеры и контрагенты

получают выгоды за счет:

- ✓ повышения защищенности ключевых бизнес-процессов;
- ✓ повышения доверия к организации со стороны контрагентов.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Снижает риски, соответственно, снижает издержки: ✓ Своевременное выявление и управление рисками. ✓ Снижение рисков от внешних и внутренних угроз. **Подчеркивается прозрачность и чистота бизнеса перед законом благодаря соответствию стандарту**	**Общество** *получает выгоду от:* выполнения законодательных и нормативных требований.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

3. Выбираем бизнес-процесс, или Как понять, что будем сертифицировать

На первый взгляд может показаться, что выбор области действия и составления перечня бизнес-процессов, которые попадают в эту самую область действия, – очень простая, незатейливая, практически тривиальная задача, но это далеко не так.

От начинающих специалистов в области ИБ или людей, которые никогда не сталкивались с вопросами безопасности, зачастую можно услышать ответ, что мы будем сертифицировать абсолютно все процессы, которые есть в компании. Зачем мелочиться?

Однако практика показывает, что сертификацию всех бизнес-процессов не всегда можно реализовать по разным причинам, например, финансовым.

Как же тогда выбирать?

До момента утверждения сертифицируемой области действия имеет смысл составить список, если хотите – чек-лист, всех существующих бизнес-процессов в компании и выбрать из него наиболее критичные процессы с точки зрения информационной безопасности. Это может быть обработка и хранение данных клиентов, финансовые операции, работа с чувствительными данными или что-то иное.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

В процессе выбора важно учесть такой внешний фактор, как запросы клиентов: в какой области деятельности вашей компании клиенты все больше интересуются наличием сертификатов на соответствие национальным и/или международным стандартам в области информационной безопасности.

В качестве наиболее действенного способа определения области действия и бизнес-процессов, которые будут сертифицироваться, мы предлагаем вам заполнить чек-лист. Он позволит наглядно представить все процессы и проранжировать их по степени значимости.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Чек-лист для определения области деятельности СУИБ компании

№ п/п	Название бизнес-процесса	Краткое описание	Участники бизнес-процесса	Какие информационные системы задействованы	Какого рода информация обрабатывается в информационных системах	На основе какой нормативной и законодательной базы работает бизнес-процесс	Критичность с точки зрения ИБ по шкале от 1 до 4*	Важность процесса с точки зрения клиента от 1 до 3 **

* где:
1 – высокая,
2 – средняя,
3 – низкая,
4 – не влияет на процесс.

** где:
1 – важен,
2 – маловажен,
3 – не важен.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Зачем заполнять этот чек-лист?

Прежде всего, для систематизации процессов. Уже на основании этого можно определить область действия и процессы, которые в нее попадают.

Дополнительно, учитывая наш опыт, такая **систематизация сэкономит вам минимум 6 месяцев** работы и соответственно денежные средства, которые будут вложены за эти полгода. Неправильный, некорректный или несогласованный выбор заставит вас начинать процесс подготовки к сертификации с самого начала.

Читайте далее и вы сможете узнать ключевые моменты, определяющие суть системы информационной безопасности и ее области деятельности.

Какова цель системы управления информационной безопасностью компании?

Система управления информационной безопасностью (СУИБ) любой компании должна быть предназначена для:

1. **Обеспечения понимания и прояснения вопросов информационной безопасности** (ИБ) работниками компании, подрядчиками, поставщиками услуг, а также другими лицами, имеющими договорные отношения с компанией (далее – сотрудники);
2. **Объединения усилий сотрудников,** направленных на обеспечение ИБ, единым методическим аппаратом и механизмом управления;
3. **Оперативного реагирования на изменение условий** функционирования информационных систем компании (обеспечение работы при нештатных ситуациях).

На какие ресурсы распространяется область действия СУИБ?

Область действия СУИБ распространяется на такие ресурсы компании, как:

1. **Информационные ресурсы**: файлы, документы на бумажных носителях, в том числе договора, соглашения с клиентами, операционные и эксплуатационные процедуры;
2. **Средства хранения и обработки информации**: рабочие станции, переносные устройства, съемные носители информации любого типа;
3. **Программное обеспечение**: операционные системы, приложения и утилиты;
4. **Вспомогательные сервисы и системы жизнеобеспечения**: каналы связи (телефония, Интернет).
5. **Персонал.**

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Каковы направления деятельности СУИБ?

Основными направлениями деятельности СУИБ являются:

1. Выявление внешних и внутренних угроз безопасности для бизнес-процессов компании.
2. Определение существующих рисков, управление ими, а также принятие решений на основе бизнес-целей компании.
3. Снижение уровня рисков и реального ущерба от инцидентов ИБ.
4. Обеспечение эффективного управления процессами, входящими в область действия СУИБ, в том числе в критических ситуациях.
5. Поиск и корректировка уязвимых мест системы ИБ компании.
6. Четкое разграничение обязанностей сотрудников в области ИБ.
7. Распределение затрат в наиболее значимые области, важные для ведения бизнеса и подвергающиеся наиболее серьезным угрозам.
8. Выработка долговременной стратегии развития системы ИБ, соответствующей тенденциям развития компании.
9. Повышение степени привлекательности компании для инвесторов и клиентов на внутреннем и внешнем рынках

Опираясь на все эти факторы, прямые и косвенные выгоды, вы легко сможете определить область действия СУИБ для компании.

Как может звучать описание области действия СУИБ?

Ниже вы найдете 5 вариантов (примеров) описания области действия СУИБ. Вам же остается действовать по аналогии.

1. Система управления информационной безопасностью в части обеспечения безопасности процессов разработки программного обеспечения.
2. Система управления информационной безопасностью в части обеспечения безопасности процессов взаимодействия с клиентами в части обработки клиентских данных.
3. Система управления информационной безопасностью в части обеспечения безопасности процессов проектирования, поставки, обслуживания и

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

мониторинга систем безопасности и слаботочных систем.

4. Система управления информационной безопасностью в части обеспечения безопасности процессов предоставления информации в области консалтинговых услуг.
5. Система управления информационной безопасностью в части обеспечения безопасности процессов предоставления услуг по управлению ИТ-инфраструктурой.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

4. Собираем команду

Мы уже упоминали ранее, что ошибочно полагать, будто для построения, внедрения и сертификации СУИБ нужен только человек, отвечающий в компании за информационную безопасность. Даже если компания принимает решение передать вопрос построения, внедрения и сертификации СУИБ на аутсорс, в любом случае в самой компании важно сформировать рабочую группу (команду), которая будет участвовать в этом процессе.

Мы не зря предложили вам заполнить чек-лист по бизнес-процессам (см. раздел № 3). Именно он поможет вам достаточно четко определить ключевые бизнес-процессы, а следовательно, и ключевых лиц, которые должны войти в команду, работающую над построением системы СУИБ и подготовкой к сертификации.

Участие в процессе построения СУИБ сотрудников разных подразделений, включенных в область действия СУИБ, – далеко не бумажная формальность. Этим людям предстоит сделать немало работы, в том числе предстоит отвечать на вопросы аудитора на финальном этапе прохождения сертификации.

В качестве наглядного примера мы приведем состав команды одного из наших реальных проектов.

В состав команды входили:

1. Директор компании.
2. Директор по финансам и развитию.
3. Секретарь как человек ответственный за работу с документами.

4. Менеджер по вопросам информационной безопасности.
5. Системный администратор.

Часто задают вопрос: **какое количество человек, входящих в состав рабочей группы по созданию и внедрению СУИБ, можно считать достаточным?**

Все зависит от размера компании и тех процессов, которые вы решили выбрать для сертификации.

Однако команда должна состоять минимум из трех человек. Эти же люди войдут в состав комиссии, будут обсуждать и принимать решения относительно проведения тех или иных мероприятий в ходе построения и внедрения СУИБ.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

5. Подготовка документов

В этом разделе мы постарались описать весь пакет документов, который должен существовать и создаваться в компании в процессе построения СУИБ и подготовки к сертификации. Что из этого создавать, а что нет – решает человек, ответственный за проект. В каждом конкретном случае и для каждой компании этот перечень будет иметь свои особенности.

> **Важно**! *Любой документ в рамках СУИБ является «живым» и должен пересматриваться по мере необходимости, но не менее 1 раза в год.*

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

5.1. Какие документы необходимо разработать

Ниже вы найдете список, содержащий минимальный набор документов, необходимых для ISO/IEC 27001 версии 2013 года:

№ п/п	Документы	Номер пункта стандарта
1.	Область действия	4.3
2.	Политика информационной безопасности	5.2, 6.2
3.	Методология оценки и обработки рисков	6.1.2
4.	Положение о применимости	6.1.3 d)
5.	План устранения рисков	6.1.3 e), 6.2
6.	Отчет об оценке рисков	8.2
7.	Процедура управления документами	7.5
8.	Процедура управления записями	7.5
9.	Порядок внутреннего аудита	9.2
10.	Порядок и устранение неисправностей	10.1
11.	Определение ролей и обязанностей	A.7.1.2, A.13.2.4
12.	Материально-технические ресурсы активов	A.8.1.1
13.	Допустимое использование активов	A.8.1.3
14.	Политика управления доступом	A.9.1.1
15.	Процессы управления IT	A.12.1.1
16.	Принципы разработки защищенной системы	A.14.2.5
17.	Политика безопасности поставщика	A.15.1.1
18.	Процедура управления инцидентами	A.16.1.5
19.	Процедуры непрерывности бизнеса	A.17.1.2
20.	Юридические, регулирующие и договорные требования	A.18.1.1

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

№ п/п	Записи*	Номер пункта стандарта
1.	Записи о степени подготовки, навыках, опыте и квалификации	7.2
2.	Мониторинг и измерение результатов	9.1
3.	Программа внутреннего аудита	9.2
4.	Результаты внутренних аудитов	9.2
5.	Результаты анализа со стороны руководства	9.3
6.	Результаты корректирующих действий	10.1
7.	Журналы пользовательских действий, исключений и событий безопасности	A.12.4.1, A.12.4.3

* Пункты из приложения А могут быть исключены из рассмотрения, если организация приходит к заключению, что нет никаких рисков или других требований для использования этой системы управления.

Приведенный список не является окончательным и может дополняться и изменяться. Стандарт предполагает определенную гибкость и позволяет использовать альтернативные документы. Добавления к текущему списку могут производиться с целью повышения уровня информационной безопасности и основываться на требованиях системы СУИБ и опыта.

В дополнение к вышеизложенному списку основных документов мы предлагаем вам перечень документов, которые очень часто используются при подготовке и построении СУИБ, но не являются обязательными с точки зрения стандарта:

№ п/п	Документы	Номер пункта стандарта
1.	Политика использования собственных устройств (BYOD)	A.6.2.1
2.	Мобильное устройство и политика удаленного доступа	A.6.2.1
3.	Политика классификации информации	A.8.2.1, A.8.2.2, A.8.2.3
4.	Парольная политика	A.9.2.1, A.9.2.2, A.9.2.4, A.9.3.1, A.9.4.3
5.	Политика уничтожения и утилизации	A.8.3.2, A.11.2.7

6.	Процедуры для работы в контролируемых зонах	A.11.1.5
7.	Политика чистого экрана и рабочего стола	A.11.2.9
8.	Политика управления изменениями	A.12.1.2, A.14.2.4
9.	Политика резервного копирования	A.12.3.1
10.	Политика передачи информации	A.13.2.1, A.13.2.2, A.13.2.3
11.	Анализ влияния на бизнес	A.17.1.1
12.	План тестирования	A.17.1.3
13.	Техническое обслуживание и обзор плана	A.17.1.3
14.	Стратегия непрерывности бизнеса	A.17.2.1

Несмотря на то что эти документы не являются обязательными с точки зрения стандарта, мы рекомендуем предусмотреть наличие этих документов в компании, так как они регламентируют ряд необходимых мер и действий, внедрение которых необходимо для построения комплексной системы СУИБ.

Одним из ключевых назначений документов из дополнительного списка (таких, как политики) есть регламентация внедрения и осуществления процессов, а также удобная форма донесения правил и норм, вводимых в компании, до сотрудников компании и до внешних организаций.

Вторым фактором для создания дополнительных документов является необходимость письменного подтверждения проведения работ, разово или на постоянной основе, требующихся в рамках построения и сопровождения системы СУИБ.

Важно! *Основной раздел стандарта является обязательным, а следовательно, все требования должны быть выполнены, в том числе разработаны все упомянутые документы.*

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

5.2. О каких документах не сказано в стандарте

Стандарт ISO 27001 не содержит в себе исчерпывающего перечня документов, так как многие требуемые документы являются внутренними распорядительными документами компании: приказы, распоряжения, протоколы, акты и т. п.

Безусловно, для крупных компаний, со сформированной системой документооборота, вопрос внутренних распорядительных документов может показаться неактуальным. Система документооборота здесь существует и, как правило, отлажена.

Для маленьких компаний задача внутренних документов может встать остро, так как здесь все привыкли решать без создания дополнительных документов. По этой причине всегда стоит подумать о внутренних документах:

1) приказ о решении создать и внедрить СУИБ;
2) приказ о назначении ответственных лиц;
3) приказ о создании комиссии по вопросам информационной безопасности;
4) протоколы заседаний этой самой комиссии и т. п.

Если у вас небольшая компания, также стоит привести в порядок/пересмотреть существующие кадровые документы (трудовые договора, должностные инструкции, приказы о приеме на работу сотрудников и т. п.).

5.3. Типовая структура документов СУИБ

Отдельно рассмотрим саму структуру документов. Будь то политика или положение о применимости, процедура и т. п.

Что должен содержать документ:

1. Цель создания документа.
2. Область действия документа, роли и обязанности задействованных лиц/сторон.
3. Ссылки на перекрестные документы.
4. Основная часть документа, содержащая саму суть политики, процедуры и т. п.

5. Раздел о пересмотре документа с указанием срока пересмотра.
6. История изменений.

5.4. С какого документа начинается создание СУИБ

После подписания директором компании приказа о решении построить и внедрить СУИБ, а также распределения ролей и ответственности в этом процессе, другими словами – создания команды, мы рекомендуем начать, как бы это странно ни прозвучало, с документа под названием «Процедура управления документами». Именно он устанавливает правила написания и оформления всех последующих документов, создавая тем самым единообразие, и облегчает последующею работу над созданием документов.

Общепринятый стандарт оформления и содержания документов предусматривает наличие такой процедуры, и у многих компаний она уже существует, хотя ее создание и не было связано с построением СУИБ. Для тех же компаний, у которых еще нет принятого внутреннего стандарта по оформлению документации, стоит начать именно с него. Поверьте, в дальнейшем это сэкономит вам время на переформатировании и переоформлении готовых документов, особенно если их созданием будут заниматься несколько человек.

5.5. Процедура управления документами и записями

Процедура управления документами обычно автономная; содержит 2 или 3 страницы, не считая титульного листа. В ней содержатся:

1. Правила форматирования документов

Например:

Текстовый документ должен быть написан с использованием шрифта Times New Roman, размер шрифта – 12. Для названия разделов (заголовков) используется 14 или 16 размер шрифта, а для заголовков второго уровня – 12.

Название документа должно содержать название организации и, в случае необходимости, отметку о конфиденциальности.

2. Описание процессов работы с разными внутренними документами различного типа

Например, управление входящими/исходящими документами:

Цель этой процедуры – корректная и однозначная обработка входящей и исходящей корреспонденции.

Процедура обработки корреспонденции состоит из двух этапов:

1. Обработка входящей корреспонденции.

2. Обработка исходящей корреспонденции.

Обработка входящей корреспонденции. Процедуре обработки входящей корреспонденции подвергается вся корреспонденция, попадающая в компанию, вне зависимости от источника ее отправления, способа доставки и получателя корреспонденции, за исключением случаев, когда обработка корреспонденции осуществляется по особым правилам, утвержденным директором компании.

Обработку входящей корреспонденции осуществляет секретарь компании или его заместитель.

Секретарь осуществляет получение и предварительную сортировку входящей корреспонденции. В день получения корреспонденции секретарь вскрывает конверты и передает для ознакомления директору компании, а также лицу или лицам (исполнителю из числа сотрудников компании), впрямую или косвенно указанных в корреспонденции.

После завершения работы с корреспонденцией исполнитель помещает корреспонденцию в папку-накопитель для хранения.

Обработка исходящей корреспонденции. Обработка исходящей корреспонденции осуществляется исполнителем, лицом, инициирующим отправку корреспонденции, и заключается в подготовке документов для отправки, присвоении уникального номера, если это требуется, и передаче для осуществления отправки секретарю компании.

Секретарь компании осуществляет отправку корреспонденции принятыми в компании способами.

3. Правила информирования сотрудников компании

Примером информирования о корреспонденции может служить следующая таблица:

Тип входящей или исходящей корреспонденции	***Информируемые сотрудники***
Проектная корреспонденция	*Директор* *Менеджер проекта* *Члены проектной команды*
Финансовые документы	*Директор* *Бухгалтер*
Маркетинговые и другие информационные материалы	*Директор* *Менеджер проекта*

4. Идентификация документов

Каждый документ в системе управления информационной безопасностью, как и документы компании в целом, имеет свой идентификационный номер, что позволяет обеспечить классификацию при хранении документов, упрощает процесс отсылки к ним и последующий поиск.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

5.6. Политика информационной безопасности

Политика информационной безопасности, как правило, является небольшим документом высшего уровня, который описывает основную цель СУИБ. Цели СУИБ обычно могут быть выделены в отдельный документ, но также они могут быть включены в политику информационной безопасности. В отличие от пересмотренного ISO 27001:2005, в новой версии стандарта нет необходимости в наличии двух документов: политики СУИБ и политики информационной безопасности – необходима только политика информационной безопасности.

Предлагаем вашему вниманию выдержки из политики ИБ, самые ключевые моменты:

Цель политики – защита информационных ресурсов компании от всех внутренних, внешних, преднамеренных или непреднамеренных угроз.

Основные положения политики ИБ:

- *Политика утверждается руководителем компании единолично или совместно с советом директоров компании.*
- *Сотрудник, ответственный за обеспечение ИБ в компании, осуществляет управление процессами информационной безопасности, обеспечивая грамотное управление информационными ресурсами.*
- *Для управления информационными ресурсами и СУИБ в компании может быть создан комитет по ИБ, обеспечивающий принятие регламентов и мер обеспечения ИБ коллегиальным способом.*
- *Сотрудник, ответственный за ИБ, ежегодно и при появлении существенных изменений проводит анализ существующих политик ИБ с целью обеспечения их постоянной пригодности, адекватности и результативности.*
- *Сотрудник, ответственный за ИБ, отвечает за определение детальных требований к системе информационной безопасности и контролирует выполнение этих требований.*
- *Доступ к информации и информационным ресурсам компании предоставляется только лицам/сотрудникам, которым этот доступ необходим для выполнения должностных или договорных обязательств. При этом уровень доступа – минимально возможный.*
- *Для каждого информационного ресурса компании определен владелец ресурса (сотрудник или подразделение), отвечающий за предоставление доступа к ресурсу и эффективное функционирование мер защиты информации, примененных для защиты ресурса.*
- *По всем фактическим или предполагаемым нарушениям информационной безопасности проводится расследование с целью определения причин наступления инцидента. В случае необходимости, к расследованию могут подключаться сторонние компании.*
- *Средства управления информационной безопасностью внедряются по результатам проведения оценки рисков информационной безопасности.*
- *В компании проводится регулярное обучение персонала в области информационной безопасности.*

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

- *В компании ежегодно проводится независимый аудит информационной безопасности, что обеспечивает актуализацию системы в целом.*
- *Компания раз в год проводит внутренний аудит информационной безопасности.*
- *В компании созданы и реализованы детальные политики и процедуры для поддержки основной политики.*
- *Компания выполняет законодательные и нормативные требования, предъявляемые к ней.*

5.7. Реестр ресурсов

Реестр ресурсов – это таблица, содержащая основную информацию обо всех ресурсах, задействованных в бизнес-процессах, которые попадают в область действия СУИБ. Составление такой таблицы необходимо для дальнейшей обработки рисков: выбор методов устранения тех или иных угроз, понижения уровня риска.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Реестр ресурсов

№ п/п	Тип ресурса	Владелец ресурса	Владелец риска	Пользователь ресурса	К	Ц	Д
	Информация						
	Оборудование (компьютерное, прикладное, сетевое)						
	Программное обеспечение						
	Сервисы (внутренние, внешние)						
	Персонал						
	Помещения						

где:

К – конфиденциальность;
Ц – целостность;
Д – доступность.

К, Ц, Д – свойства информации, которые важны для каждого типа ресурса с точки зрения информационной безопасности. Проставляются знаками «+» и «-» (как вариант можно ставить 1 или 0).

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

5.8. Методология оценки и обработки рисков, отчет

Методология оценки и обработки рисков, как правило, представляет собой документ объемом от 4 до 5 страниц, который должен быть написан до выполнения процедур оценки и обработки рисков. Отчет об оценке степени риска пишут после того, как выполняются процедуры оценки степени риска и обработки риска. Этот отчет должен суммировать все результаты.

Как оценивать риски?

Существует множество методов оценки и обработки рисков. Здесь мы предлагаем рассмотреть так называемый качественный метод.

Первоначально необходимо определить шкалы ценности ресурсов, например от 1 до 4:

Ценность ресурса	***Описание***
1	*Утрата конфиденциальности, и/или ценности, и/или доступности ресурса практически не приводит к последствиям с финансовыми потерями.*
2	*Утрата конфиденциальности, и/или ценности, и/или доступности ресурса приводит к незначительным финансовым потерям и оказывает незначительное влияние на репутацию компании.*
3	*Утрата конфиденциальности, и/или ценности, и/или доступности ресурса приводит к значительным финансовым потерям и имеет значительное влияние на репутацию компании.*
4	*Утрата конфиденциальности, и/или ценности, и/или доступности ресурса приводит к большим финансовым потерям (определить сумму), имеет значительное влияние на репутацию компании и может привести к остановке работы бизнес-процесса.*

Далее определяемся со шкалой степени уязвимости ресурса компании с точки зрения информационной безопасности:

Степень уязвимости	***Описание***
1	*Уязвимость практически не приводит к раскрытию конфиденциальной информации.*
2	*Уязвимость приводит к раскрытию сведений, которые относятся к коммерческой тайне, персональным данным, и приводит к финансовым потерям.*
3	*Уязвимость приводит к раскрытию сведений, которые относятся к коммерческой тайне, персональным данным, и приводит к значительным финансовым потерям, имеет значительное влияние на репутацию компании и может привести к остановке работы бизнес-процесса.*

Степень уязвимости	*Описание*
4	*Приводит к остановке бизнес-процесса и нарушению закона.*

Кроме того, необходимо учесть такой факт, как вероятность возникновения той или иной угрозы. В качестве шкалы для оценки вероятности реализации угроз возьмем шкалу от 1 до 4:

Оценка вероятности	*Описание*
1	*Угроза имеет место в историческом аспекте.*
2	*Угроза возникает 2-3 раза в год по отрасли.*
3	*Угроза имела место 1 раз в компании.*
4	*Угроза проявляется 2-3 раза в год в компании.*

Заметим, что в таком случае вероятность не имеет ничего общего с математическим понятием «вероятность».

Оцениваем уровень риска

Уровень риска по отдельным парам угроза/уязвимость, которая может использоваться для реализации этой угрозы, определяется перемножением значений ценности ресурса, его степени уязвимости и вероятности реализации угрозы:

$$\mathbf{Р = ЦН \times СУ \times В,}$$

где:
ЦН – ценность актива;
СУ – степень уязвимости ресурса (оценивается по шкале от 1 до 4, исходя из текущей ситуации с этим ресурсом);
В – вероятность реализации угрозы.

Общий уровень риска для ресурса СУИБ компании равен максимальной величине из всех рисков по каждой паре угроза/уязвимость (для этого ресурса СУИБ компании).

Заносим данные в таблицу «Отчет об оценке рисков для ресурсов СУИБ компании».

Отчет об оценке рисков для ресурсов СУИБ компании

Ресурс	Угрозы	Уязвимости	ЦН	СУ	В	Р

Как определить: какие риски обрабатываем, а какие принимаем?

Итак, мы составили список ресурсов, определили для каждого такой параметр, как ценность, степень уязвимости и вероятность возникновения той или иной угрозы при существующем уровне уязвимости и рассчитали риск.

Например:

Ресурс	***Угрозы***	***Уязвимости***	***ЦН***	***СУ***	***В***	***Р***
Компьютер XXX	*НСД*	*Свободный доступ к рабочему месту*	*3*	*3*	*2*	*18*

Чтобы определить критерии принятия решения относительно каждого отдельного риска, составляется шкала, например:

Условное обозначение риска	**Числовое значение оценки риска***	**Решение относительно дальнейшей обработки риска**
Низкие риски	1–10	Риск считается незначительным. Обработка рисков не требуется.
Средний риск	11–21	Обработка риска может выполняться или не выполняться.
Высокий риск	22–64	Риск считается существенным. Обработка рисков обязательна.

* колонка содержит значения, соответствующие оценке риска.

Компания принимает для себя, что риски выше 10 подлежат обработке и принятию мер с целью понижения уровня риска.

5.9. Положение о применимости

Положение о применимости (еще его называют SOA) пишется на основе результатов обработки риска. Это центральный документ в СУИБ, потому что он описывает не только средства, которые будут использоваться для Приложения А, но и то, как они будут реализованы, и их текущий статус. Также можно рассматривать Положение о применимости в качестве документа, описывающего Профиль безопасности вашего предприятия.

Положение о применимости представляет собой таблицу из приложения А стандарта с определенными правилами заполнения.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Название столбцов в таблице:

1. Номер пункта в приложении А к стандарту. При использовании дополнительных мер безопасности, которые не указаны в приложении А стандарта, используется своя нумерация.

Пример заполнения: А.5.1.1; А.12.3

2. Название пункта контроля.
3. Описание пункта контроля.
4. Отметка о применимости.

Примеры заполнения: Да, Нет;

5. Причина исключения. Эта колонка заполняется в случае значения отметки относительно применимости «Нет».
6. Метод реализации. Эта колонка описывает метод реализации контроля.

Далее мы приводим выдержки из этого документа:

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

№ контроля	Название контроля	Описание контроля	Применимость контроля (Да/Нет)	Причина исключения контроля	Метод реализации
A.5	Политика безопасности				
A.5.1	Политика информационной безопасности				
A.5.1.1	Документированная политика информационной безопасности	Политика информационной безопасности должна быть утверждена руководством, издана и доведена до сведения всех сотрудников организации, а также сторонних организаций	Да		Политика системы управления информационной безопасностью
A.5.1.2	Пересмотр политики информационной безопасности	Политика информационной безопасности организации должна быть подвергнута анализу и пересмотру через заданные промежутки времени или при появлении существенных изменений характеристик целей безопасности	Да		Политика системы управления информационной безопасностью
A.6	Организация информационной безопасности				
A.6.1	Внутренняя организация				
A.6.1.1	Роли и ответственность в рамках информационной безопасности	Все ответственности в поле информационной безопасности должны быть определены и закреплены.	Да		Обязанности персонала по обеспечению ИБ перечислены в различных документах СУИБ
A.6.1.2	Распределение обязанностей по обеспечению информационной безопасности	Противоречивые обязанности и зоны ответственности должны быть разделены с целью снижения возможностей для несанкционированного, случайного изменения или неправильного использования активов организации.	Да		Обязанности персонала по обеспечению ИБ перечислены в различных документах СУИБ
A.6.1.3	Контакт с органами власти	Должны поддерживаться соответствующие контакты с соответствующими органами власти	Да		План обеспечения непрерывности бизнеса
A.6.1.4	Контакт с профессиональными объединениями	Должны поддерживаться необходимые контакты с профессиональными объединениями или другими форумами специалистов по безопасности и профессиональными ассоциациями	Да		Обучение специалистов в области ИБ, участие в вебинарах, конференциях, форумах по ИБ

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

№ контроля	Название контроля	Описание контроля	Применимость контроля (Да/Нет)	Причина исключения контроля	Метод реализации
A.6.1.5	Информационная безопасность при управлении проектами	Информационная безопасность должна обеспечиваться при управлении проектами независимо от типа проектов	Да		Политика аудита информационной безопасности, Сертификационный аудит от BSI
A.11	Физическая безопасность и безопасность окружающей среды				
A.11.1	Защищенные области				
A.11.1.1	Физический периметр безопасности	Для защиты зон, содержащих информацию и средства ее обработки, должны использоваться периметры безопасности (различные барьеры, такие как стены, проходные с контролем доступа по картам, приемные с дежурными)	Да		Вход на территорию здания, в котором расположен офис компании, ограничен автоматически запираемой решеткой и постом охраны на входе
A.11.1.2	Механизмы контроля физического входа	Защищенные области должны быть защищены соответствующими механизмами контроля входа, обеспечивающими возможность доступа только для авторизованного персонала	Да		Доступ в офис производится только по пропускам и документам, удостоверяющим личность
A.11.1.3	Защита офисов, комнат и оборудования	Должны проектироваться и применяться механизмы обеспечения физической безопасности офисов, комнат и оборудования	Да		Офисное помещение запирается на ключ
A.11.1.4	Защита от внешних угроз и угроз со стороны окружающей среды	Должна проектироваться и применяться физическая защита от ущерба, вызванного огнем, наводнением, землетрясением, взрывом, гражданскими беспорядками и другими формами природных и антропогенных катастроф	Да		В помещении расположена пожарная сигнализация, окна плотно закрываются, вход на территорию ограничен
A.11.1.5	Работа в защищенных областях	Должны проектироваться и применяться механизмы обеспечения физической безопасности и инструкции по работе в защищенных областях	Нет	Компания не проводит подобных работ	
A.11.1.6	Область общего доступа, доставки и погрузки	Места доступа, такие как область приема, отгрузки материальных ценностей, и другие места, где неавторизованные лица могут проникнуть в помещения, должны быть под контролем и по возможности должны быть изолированы от средств обработки информации во избежание несанкционированного доступа	Нет	В офисе нет зоны общего доступа	

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

5.10. План устранения рисков

В основном он является планом действий по реализации различных элементов управления, определенных Положением о применимости, разрабатывается на основе заявления о применимости, активно используется и обновляется по мере внедрения СУИБ. Иногда он может быть включен в проектный План.

План по обработке рисков представляет собой таблицу, которая выглядит следующим образом:

Тип ресурса	Угрозы	ЦН	СУ	В	Р	ПР	Планируемые контрмеры	ОР	Срок реализации контрмеры	Ответственный

ЦН – ценность актива;
СУ – степень уязвимости ресурса (оценивается по шкале от 1 до 4, исходя из текущей ситуации с этим ресурсом);
В – вероятность реализации угрозы;
Р – уровень риска;
ПР – приемлемый уровень риска;
ОР – остаточный уровень риска.

5.11. Политика контроля доступа

Этот документ определяет правила доступа как к физическим объектам, так и к логическим. Обычно создается после окончания оценки рисков и процессов обработки рисков.

Пример содержания этого документа приведен ниже.

Получение доступа к информационным ресурсам компании

Доступ *к информационным ресурсам компании, содержащим конфиденциальную информацию, предоставляется сотрудникам* ***после подписания*** *Договора о неразглашении конфиденциальной информации.*

Для создания учетной записи новому сотруднику (пользователю) *во всех необходимых для работы информационных ресурсах руководитель сотрудника направляет письменный запрос на корпоративный электронный адрес системного администратора и сотрудника, ответственного за ИБ, с указанием перечня необходимых ресурсов и уровня доступа (пользователь, пользователь с административными правами и т. п.) к этим ресурсам. После получения подтверждения от сотрудника, ответственного за ИБ, системный администратор создает необходимые учетные записи и присваивает необходимый уровень прав.*

В случае необходимости изменения прав доступа *к информационным ресурсам для выполнения служебных обязанностей руководитель сотрудника направляет запрос на корпоративную электронную почту системного администратора и сотрудника, ответственного за ИБ, с указанием причины внесения изменений, названия ресурса и требуемого уровня доступа. Изменения в учетную запись вносятся системным администратором после получения письменного подтверждения от сотрудника, ответственного за ИБ.*

Все спорные ситуации относительно предоставления доступа решаются через директора компании.

Возвращение ресурсов компании по окончании договора

В случае увольнения и/или расторжения договора *сотрудник компании обязан незамедлительно вернуть все информационные ресурсы, которые ему были предоставлены для выполнения работ (оказания услуг), а также все носители информации, которые содержат конфиденциальную информацию компании или ее клиентов, их копии, рукописи, черновики, схемы, чертежи, магнитные ленты, фотографии, диски, дискеты, распечатки на принтере, кино-, фотонегативы и другие носители информации.*

Использование корпоративной сети и сети Интернет

Пользователь не должен читать, изменять, удалять или копировать любые файлы, принадлежащие другим пользователям, не получив предварительно разрешения от владельца файла. Если явно не установлен доступ для всех пользователей, как это имеет место в совместно используемых каталогах, возможность считывать, изменять, удалять или копировать файлы, принадлежащие другим пользователям, не означает разрешения на выполнение этих действий.

Пользователь не должен использовать уязвимости в защите информационных систем для нанесения ущерба этим системам, осуществления несанкционированного доступа к хранящейся в них информации, использования приложений, не имеющих отношения к выполнению их функциональных обязанностей, использования информационных ресурсов, выделенных другим пользователям.

Пользователю запрещается использовать ресурсы корпоративной сети компании для получения несанкционированного доступа к любым другим сетям (системам), не принадлежащим компании, или каким-либо образом создавать помехи, изменять либо нарушать функционирование этих систем.

Пользователю запрещается предпринимать действия для получения паролей, ключей шифрования и любых других данных, которые могут быть использованы для получения несанкционированного доступа к информационным ресурсам корпоративной сети компании.

Подключение корпоративной сети (отдельных участков корпоративной сети, систем, подключенных к корпоративной сети, и т. п.) компании к сети Интернет осуществляется только через средства разграничения доступа в виде межсетевых экранов (МЭ). Не допускаются любые подключения корпоративной сети к сети Интернет в обход МЭ.

Установка и изменение конфигурации клиентского программного обеспечения, предназначенного для взаимодействия с сетью Интернет, выполняется только системными администраторами компании. Пользователь не имеет права производить самостоятельную установку и/или модификацию указанного программного обеспечения.

Ответственность за использование не прошедшего экспертизу и не рекомендованного к использованию программного обеспечения целиком и полностью возлагается на пользователя, использующего такое программное обеспечение. При обнаружении системными администраторами фактов такого рода использования производится отключение рабочего места сотрудника от сети Интернет, а также уведомляют о нарушении руководителя сотрудника и сотрудника, ответственного за ИБ.

При предоставлении пользователю информационных сервисов компания исходит из принципа минимизации привилегий. Тем пользователям, которым не требуются услуги сети Интернет для осуществления деятельности в рамках исполнения своих обязанностей, доступ к сети Интернет не предоставляется.

Доступ к сети Интернет по протоколам SMTP, POP3, IMAP4 предоставляется только в исключительных случаях и требует специального согласования. Доступ по протоколам Telnet и SSH может предоставляться только системным администратором компании.

5.12. Операционные процедуры управления ИТ

Под операционными процедурами подразумеваются такие процедуры управления, как управление изменениями, сторонние услуги, резервное копирование, сетевая безопасность, вредоносный код, удаление и уничтожение, передача информации, система контроля и т. д.

Эти процедуры могут быть написаны как в виде единого документа, так и в виде серии политик и процедур. Если у вас небольшая компания, то, как правило, все эти политики и процедуры могут быть объединены в единый документ.

Все эти политики и процедуры, как правило, пишутся только после того, как вы закончите оценку и обработку рисков.

5.13. Записи обучения, навыков, опыта и квалификаций

Обычно эти записи хранятся в отделе кадров. Если у вас нет такого отдела, то эти обязанности возлагаются на соответствующего сотрудника. Таким образом, в организации должна содержаться папка со всеми документами, подтверждающими факт обучения и повышения квалификации каждого сотрудника.

Также хорошей практикой считается наличие годового плана обучения сотрудников вопросам информационной безопасности, создание справочников с выдержками ключевых моментов из политик и процедур.

Обучение сотрудников может проводить непосредственно человек, ответственный за информационную безопасность. На таком занятии могут рассматриваться текущие новости и события в области информационных технологий. Периодичность таких занятий компания устанавливает самостоятельно. Оптимальный вариант – раз в месяц. Если же по каким-то причинам это затруднительно, постарайтесь проводить подобного рода мероприятия хотя бы раз в квартал.

Еще один немаловажный момент – тестирование. Необходимо регулярно проводить тестирование сотрудников на знание политик и процедур.

5.14. Кратко о Непрерывности бизнеса

Несмотря на существование отдельного стандарта на эту тему, в ISO 27001 также присутствуют контроли, посвященные непрерывности бизнеса.

По сути, необходимо предусмотреть наличие инструкций на случай чрезвычайных ситуаций, таких как пожар, наводнение, отсутствие электроэнергии, недоступность каналов связи и т. п.

Безусловно, для каждой компании перечень факторов, влияющих на непрерывность бизнеса, будет своим. Важно, чтобы помимо инструкции на случай чрезвычайной ситуации, у вас была методика проведения учений с персоналом и акт, подтверждающий проведение учений по факту реагирования в случае чрезвычайных ситуаций.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

6. Выходим на финишную прямую – сертификационный аудит

Итак, вы определились с областью сертификации, подготовили все необходимые документы, внедрили организационные и технические меры, самостоятельно проверили работоспособность СУИБ (провели внутренний аудит).

Когда же приглашать аудитора? Аудитора стоит приглашать, если с момента построения и внедрения СУИБ прошло не меньше полугода. Для аудиторов это, прежде всего, признак хорошего тона, да и вы за это время успеете отследить недочеты в системе, внести корректировки.

Какие существуют варианты проведения аудита?

Существует два варианта проведения аудита:

1. Предварительный аудит + сертификационный.
2. Сертификационный.

В первом варианте первоначально проводится предварительный аудит, который отличается от сертификационного тем, что в случае выявления несоответствий стандарту у

вас будет время внести корректировки и выйти на сертификационный аудит более подготовленными.

Между предварительным и сертификационным аудитом, согласно регламенту BSI, должно пройти не менее одного месяца.

Если ваша СУИБ давно и надежно функционирует, вы полностью уверены в своих силах, то можете сразу проходить сертификационный аудит.

Куда обращаться относительно проведения аудита?

По вопросам проведения сертификационного аудита вам следует обратиться в региональное представительство BSI. Контакты можно посмотреть на официальном сайте: http://www.bsigroup.com/ru-RU/

Как проходит сертификационный аудит?

Сертификационный аудит состоит из двух основных этапов:

1. Изучение документации.
2. Диалог с сотрудниками, входящими в область действия СУИБ.

Длительность каждого из этапов зависит от размера компании.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

7. Продолжительность процесса по построению, внедрению и сертификации СУИБ

Итак, вы решили начать процесс построения, внедрения и сертификации СУИБ. Зная количество сотрудников компании, вы можете приблизительно оценить, сколько времени займет вся эта процедура:

- ✓ Для компаний с численностью меньше чем 10 сотрудников – **до 4 месяцев**.
- ✓ Для компаний с численностью 10–50 сотрудников – **до 8 месяцев**.
- ✓ Для компаний с численностью 50–500 сотрудников – **до 12 месяцев**.
- ✓ Для компаний с численностью 500 или больше сотрудников – **до 18 месяцев**.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

8. Стоимость реализации

Невозможно вычислить стоимость до того, как оценка степени риска будет завершена и будут идентифицированы применяемые средства управления. Большинство инвестиций обычно требуют не технологии, а сотрудники, которые реализуют СУИБ (инвестированное время + обучение).

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

9. Что выбрать: аутсорсинг или самостоятельное построение и внедрение СУИБ?

Для ответа на этот вопрос рассмотрим основные преимущества каждого из способов.

Внедрение системы управления информационной безопасностью может обеспечить следующие преимущества:

1. Демонстрация защиты внутренних средств управления и соответствие требованиям корпоративного руководства и непрерывности бизнес-процессов.
2. Соблюдение действующих законов и нормативных актов.
3. Обеспечение конкурентных преимуществ, благодаря точному исполнению требований договоров, а также демонстрация того, что защита информации клиентов является первостепенной задачей компании.
4. Независимое подтверждение того, что риски организации должным образом выявлены, оценены и находятся под контролем, процессы формализованы, процедуры и документация, относящиеся к обеспечению информационной безопасности, разработаны и поддерживаются.
5. Доказательство стремления руководства к обеспечению информационной безопасности компании.
6. Регулярная оценка помогает постоянно контролировать эффективность и внедрять улучшения.
7. Повышение компетентности персонала в области ИБ. (Большое количество инцидентов ИБ связано с человеческим фактором. Поэтому важно, чтобы персонал понимал необходимость обеспечения ИБ. СУИБ включает в себя управление человеческими ресурсами. Это позволяет поддерживать необходимый для бизнеса уровень компетенции сотрудников в вопросах ИБ.)

- ✓ Доведение памяток по ИБ;
- ✓ Разработка портала по ИБ;
- ✓ Обучение по ИБ;
- ✓ Тестирование и анкетирование по ИБ;
- ✓ Интеграция с системой аттестации персонала;
- ✓ Стратегическая экономия средств;
- ✓ Меньше ресурсов и вложений в ИБ;
- ✓ Проще пройти проверку регуляторов (ИТ-аудит сопровождения);
- ✓ Экономия времени, ресурсов и затрат.

Передавая процессы управления информационной безопасностью на аутсорсинг, организация получает следующие основные преимущества:

1. **Экономия времени и средств на внедрение этих процессов управления в организации** (процессы управления стартуют сразу же после заключения соответствующего соглашения об уровне сервиса в полном объеме; для их реализации используется уже готовая методология и инструментарий).
2. **Достижение более высокого уровня качества и эффективности процессов управления** (использование высококвалифицированных специалистов внешних организаций).
3. **Существенное сокращение операционных расходов на обеспечение информационной безопасности** (стоимость аутсорсинга, как правило, не превышает расходов на заработную плату одного штатного специалиста соответствующей квалификации, которого организация может нанять для реализации соответствующих процессов управления безопасностью).
4. **Значительная экономия на соответствующих технических и программных средствах** (использование существующих инструментальных средств для проведения инвентаризации ресурсов, оценки рисков, оценки соответствия требованиям стандартов, разработки политик и регламентов, планирования процессов внутреннего аудита, подготовки отчетности и т. п.).
5. **Потенциально более высокая степень независимости и объективности внешних специалистов.**

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Таким образом, на основании проведенного анализа основных преимуществ каждого из рассматриваемых способов можно сделать вывод, что аутсорсинг позволяет сократить начальные расходы и значительно сэкономить время на внедрение процессов управления в организации. Также при аутсорсинге используются уже существующие инструментальные средства и квалифицированные специалисты из внешних организаций.

Самостоятельное построение и внедрение системы управления информационной безопасностью требует значительных затрат на начальном этапе, но позволяет сократить расходы в дальнейшем. Также внедрение СУИБ позволяет повысить компетентность персонала в области информационной безопасности и обеспечивает независимость от внешних организаций.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

10. ТОП-10 основных ошибок при подготовке к сертификации

Наша практика проведения подготовки компаний к сертификации позволяет с уверенностью говорить, что в этом процессе все делают одни и те же ошибки. Однажды мы сами их совершили и теперь хотим, чтобы идущие за нами не повторяли их.

Мы выделили 10 самых распространенных ошибок в области подготовки, внедрения и сертификации системы управления информационной безопасностью на соответствие международному стандарту ISO 27001.

ТОП-10 основных ошибок при подготовке к сертификации:

1. Устойчивое мнение, что для соответствия ISO 27001 необходимо подготовить всего лишь пакет документов. Главное, чтобы документы были в порядке.

Мнение очень распространенное и очень коварное, так как соответствие ISO – это не только документы, но и внедрение технических и организационных мер, а главное – это непрерывная работа по развитию и поддержанию системы информационной безопасности компании круглогодично.

2. Работа по приведению в соответствие стандарту без детального плана. Нет

однозначного понимания кто, что, когда и какими средствами достигает требуемого результата.

К сожалению, многие специалисты по информационной безопасности не до конца и не в полном объеме могут оценить, какие ресурсы и в каком объеме потребуются для реализации процесса внедрения стандарта. Здесь мы говорим не только о деньгах на возможно требующуюся замену или дополнение оборудования, лицензии, но и ресурсы временные, человеческие. Здесь, конечно, помощник – только опыт.

3. Безопаснику не нужна команда, безопасник – это «человек-пароход».

Часто думаем: так сложилось исторически, что человек, отвечающий за информационную безопасность в компании, все и всегда делает сам. Сам проводит аудит, сам находит решение и сам же его внедряет. Однако один в поле не воин, так как все объять невозможно и быть спецом во всем – тоже. Другими словами, невозможно быть хорошим безопасником и разбираться в тонкостях ведения бухгалтерии, куда какие данные перетекают, кому доступ нужен и в каком объеме.

4. Неправильно выбранная область сертификации.

Выбор области сертификации можно считать самым важным шагом в процессе подготовки к сертификации. Судя по нашему опыту, здесь, как правило, возникают две ситуации. Первая – клиент хочет сертифицировать все процессы от и до, что представляет собой сложную и дорогую, а порой ненужную задачу. Другая крайность – выбирается бизнес-процесс, который ну никак нельзя назвать ключевым. В итоге процесс подготовки и сертификации становится жутко долгим и дорогим или сертифицируется то, что не нуждается в этом.

5. Сотрудники и так все знают и все понимают.

Уж так сложилось, что наша вера в ответственность и самосознание сотрудников безгранична. Мы верим, что они все понимают, сами ищут ответы на свои вопросы, а если нужно, то сами инициативно спрашивают и требуют обучения. Увы, все

не так ☹ Процесс донесения необходимости новых правил и смены привычек в работе с информацией требует усилий, сломанных копий, кнута и пряника.

6. Забываем о местном законодательстве.

Погружаясь в ISO и делая все так, как это рекомендовано в учебнике, мы в какой-то мере отрываемся от жизни, забывая о второй стороне процесса сертификации, а именно – о соответствии нашему законодательству. Одно другому не должно противоречить, и исполнять нужно оба требования одновременно.

7. Зачем нам нужна лицензия на ПО?

Лицензии на программное обеспечения, начиная с ОС, антивируса, и заканчивая серверными платформами, – это первый маркер готовности вашей компании к процессу сертификации. Если для вас лицензии – это роскошь, излишество или совсем непонятно что, то сертификацию следует отложить. Не может компания сертифицироваться на соответствие международному стандарту безопасности, если пиратские версии программного обеспечения – норма бизнеса. Это как незакрытый черный ход при бронированной входной двери.

8. Внедрение мер без тестирования.

Подготовка к сертификации наверняка потребует новых внедрений – технических или организационных. Каждое такое внедрение требует тестирования, так как невозможно все предвидеть, дать полную гарантию, что все пройдет гладко, особенно если нововведения затрагивают персонал. На своей практике мы встречали случаи, когда изменение в политике доступа к ресурсам приводило к массовому недовольству и саботажу со стороны сотрудников. Все мы – рабы своих привычек.

9. Непрерывность бизнеса – это не к нам.

Непрерывность бизнеса – то, о чем у нас всегда забывают, по крайней мере, такой вывод позволяет сделать наш опыт.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

10. Не провели внутренний аудит перед сертификацией.

По большому счету, это перепроверка, но перепроверка важная, так как только она сможет дать вам ответ на вопрос: внедрены и работают ли те механизмы, правила и корректировки, которые потребовались для соответствия стандарту? В нашей практике бывали случаи, когда в замечания по сертификации попадало то, что, как казалось, было устранено. Но, увы, кто-то забыл, отложил или саботировал.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

11. Нужно больше информации?

Для получения дополнительной информации о построении, внедрении и сертификации СУИБ обращайтесь по телефону:

+7 (495) 972 98 26.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

12. Еще о документах

В приложении 1–4 вы найдете шаблоны ряда документов, которые буду вам полезны при подготовке к сертификации.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Приложение 1

Утверждаю
Директор КОМПАНИИ
ФИО
_____
"___" _____ 20___ г

План проекта
по внедрению системы управления информационной безопасностью

Регистрационный номер документа

Версия

Дата вступления в силу

Подготовлен

Место хранения документа в электронном виде

Москва
20__

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

История изменений

Дата	Версия	Автор изменений	Описание изменений

1. Цель, сфера применения

Цель данного проекта – определить цели системы управления информационной безопасностью (СУИБ), документы, которые будут написаны, сроки, роли и обязанности в проекте.

План проекта применяется ко всем видам деятельности, осуществляемых при реализации проекта СУИБ.

Пользователями этого документа являются руководство КОМПАНИИ и члены команды проекта.

2. Перекрестные документы

Международный стандарт ISO/IEC 27001.

3. План внедрения системы управления информационной безопасностью

Цель проекта

Реализация Системы управления информационной безопасностью в соответствии с ISO 27001.

Результаты проекта

В ходе реализации проекта СУИБ планируется создать следующие документы (некоторые из них могут содержать приложения, которые прямо не указаны здесь):

1. Процедура управления документами (процедура определяет основные правила написания, утверждения, распространения и обновления документов и записей).
2. Область действия системы управления информационной безопасностью.
3. Политика информационной безопасности (это ключевой документ, используемый для управления информационной безопасностью).
4. Методологии оценки и обработки рисков (описывают методологию управления информационными рисками).
5. Реестр ресурсов (документ, содержащий перечень ресурсов, входящих в область действия СУИБ).
6. Отчет об оценке рисков (таблица является результатом оценки ценности ресурсов, а также содержит соответствующий перечень угроз и уязвимостей по каждому ресурсу, входящему в область деятельности СУИБ).
7. План обработки рисков (таблица, в которой соответствующие меры контроля безопасности выбираются для каждого неприемлемого риска).
8. Положение о применимости (документ, который определяет цели и применимость каждого контроля в соответствии с приложением А к ISO 27001).
9. Процедура проведения внутреннего аудита (определяет процедуру проверки, а также предоставления результатов).

10. Процедура корректирующих и превентивных мер (описывает процесс выполнения корректирующих и предупреждающих действий).

Могут быть составлены другие документы, которые будут необходимы в процессе построения и внедрения СУИБ.

Сроки

Сроки создания отдельных документов в ходе построения СУИБ:

Документ	Срок создания
Процедура управления документами	до xx.xx.20__
Область действия системы управления информационной безопасностью	до xx.xx.20__
Политика информационной безопасности	до xx.xx.20__
Методологии оценки и обработки рисков	до xx.xx.20__
Реестр ресурсов	до xx.xx.20__
Отчет об оценке рисков	до xx.xx.20__
План обработки рисков	до xx.xx.20__
Положение о применимости	до xx.xx.20__
Политика проведения внутреннего аудита информационной безопасности	до xx.xx.20__
Процедура корректирующих и превентивных мер	до xx.xx.20__

Финальная презентация результатов проекта запланирована на xx.xx.20__.

Организация проекта

Менеджер проекта

Роль менеджера проекта заключается в обеспечении проекта необходимыми ресурсами, согласованием с руководством внедряемых процессов и процедур, а также в проведении административных работ, связанных с проектом. Полномочия менеджера проекта должны быть такими, чтобы обеспечить бесперебойную реализацию проекта в установленные сроки.

Менеджером проекта назначается ФИО – ответственный за информационную безопасность в КОМПАНИИ.

Команда проекта

В качестве команды проекта выступают все сотрудники КОМПАНИИ. Роль команды проекта заключается в оказании помощи менеджеру проекта в различных аспектах реализации проекта по построению и внедрению СУИБ.

Основные риски проекта

Основными рисками в реализации проекта являются:

1. Продление сроков на этапе оценки рисков.
2. Продление сроков в ходе разработки пакета документов, регламентирующих процессы компании.
3. Выполнение мероприятий, которые несут ненужные расходы и временные затраты.

4. Выбор слишком дорогих мер для реализации контроля.

Менеджер проекта следит, чтобы все мероприятия в рамках проекта выполнялись в пределах определенных сроков, и в случае необходимости привлекает к решению спорных вопросов руководство компании.

Инструменты для реализации проекта, отчетность

Все документы, подготовленные в ходе проекта, будут находиться в _____*(указать местонахождение документов*). Все члены команды проекта будут иметь доступ к этим документам. Вносить изменения и удалять файлы будет разрешено только менеджеру проекта.

4. Срок действия

Этот документ вступает в силу с момента утверждения директором КОМПАНИИ. План пересматривается по мере необходимости, но не менее одного раза в год. Причинами внесения изменений в документ могут быть изменения в подходах компании к оценке рисков, а также изменения в законодательных, регуляторных и других нормах.

Ответственный за ИБ

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Приложение 2

Утверждаю
Директор КОМПАНИИ
ФИО
_____
"___" _____ 20___ г

Методика проведения оценки состояния системы управления информационной безопасностью

Регистрационный номер документа

Версия

Дата вступления в силу

Подготовлен

Место хранения документа в электронном виде

Москва
20__

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

История изменений

Дата	Версия	Автор изменений	Описание изменений

1. Цели проведения оценки состояния системы управления информационной безопасностью

Настоящая Методика проведения оценки состояния системы управления информационной безопасностью КОМПАНИИ (далее – Методика) разработана в соответствии с требованиями Международного стандарта ISO/IEC 27001 и определяет особые требования по организации и проведению оценки состояния системы управления информационной безопасности (далее – СУИБ).

Оценка проводится ежегодно с целью проверки того, что цели контроля, механизмы контроля, процессы и процедуры СУИБ:

1) соответствуют требованиям международного стандарта ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования», а также соответствуют требованиям законодательства Российской Федерации;

2) соответствуют идентифицированным во внутренних нормативных документах КОМПАНИИ (далее – компания) требованиям информационной безопасности;

3) эффективно реализованы и сопровождаются ответственными сотрудниками;

4) выполняются должным образом.

2. Область применения

Этот документ применим ко всей сфере управления информационной безопасностью (СУИБ), т. е. для всех информационных систем и других информационных ресурсов, используемых в сфере СУИБ.

Пользователями этого документа являются все работники, подрядчики, поставщики услуг, а также иные лица, работающие с информацией, принадлежащей компании, в рамках заключенных договором (далее – сотрудники).

Работник, осуществляющий Оценку (далее – Проверяющий), назначается приказом директора из числа работников компании, обладающих знаниями и навыками проведения Оценки.

При необходимости для проведения Оценки могут назначаться несколько сотрудников. В таком случае один из работников назначается руководителем группы Оценки.

3. Ответственность

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Настоящая Методика обязательна для исполнения всеми работниками, осуществляющими оценку состояния СУИБ (далее – Оценка).

Несоблюдение требований настоящей Методики влечет ответственность в соответствии с внутренними нормативными документами.

4. Перекрестные документы

ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования».

5. Порядок организации и проведения оценки состояния системы менеджмента информационной безопасности

Деятельность по организации и проведению Оценки состоит из следующих мероприятий:

1) инициирование проведения Оценки:

a) определение возможности проведения Оценки;

b) согласование проведения Оценки с директором компании;

2) подготовка к проведению Оценки:

a) издание приказа о проведении Оценки за подписью директора компании;

b) утверждение Плана проведения Оценки;

c) подготовка рабочих документов для проведения Оценки (вопросников, чек-листов и т. п.);

3) проведение Оценки:

a) проведение анализа внутренних нормативных документов компании в рамках проводимой Оценки;

b) проведение анализа внутренних нормативных документов компании в рамках проводимой Оценки;

c) взаимодействие между задействованными в проведении Оценки подразделениями;

d) сбор и верификация информации;

e) формирование результатов Оценки;

4) подготовка и распространение отчета об Оценке (далее – Отчет):

a) подготовка Отчета;

b) разработка плана корректирующих мер (далее – План) по выявленным в ходе оценки несоответствиям требованиям международного стандарта ISO/IEC 27001:2005 «Информационные технологии – Методы обеспечения безопасности – Системы управления информационной безопасностью – Требования», законодательной или нормативной базы, внутренних нормативных документов компании;

c) согласование Отчета и Плана с задействованными в Оценке сотрудниками;

d) доклад результатов Оценки компании;

e) утверждение директором компании Отчета и Плана;

f) доведение Отчета и Плана до сведения задействованных в Оценке сотрудников;

g) занесение информации об Оценке в базу данных регистрации проверок информационной безопасности;

h) последующий контроль исполнения Плана.

Согласование Отчета и Плана с задействованными в Оценке сотрудниками осуществляется следующим образом:

1) Отчет и План предоставляются для согласования задействованным в Оценке сотрудникам. Срок согласования Отчета и Плана с учетом внесения изменений и уточнений должен составлять не более трех рабочих дней с момента их получения задействованными в Оценке сотрудниками;

2) в отведенный на согласование срок задействованные в Оценке сотрудники согласовывают Отчет и План либо, в случае наличия возражений, предоставляют Проверяющему замечания в письменном виде;

3) Проверяющий рассматривает замечания, предоставленные задействованными в Оценке сотрудниками, в течение одного рабочего дня с момента их получения и вносит в Отчет и План;

4) при возникновении неразрешимых разногласий в результатах проверки между Проверяющим и задействованным в Оценке сотрудником составляется протокол разногласий, который выносится на рассмотрение директора компании;

5) в случае, когда задействованный в Оценке сотрудник в отведенный на согласование срок не согласовывает Отчет и План, но и не предоставляет замечания в письменном виде, Отчет и План признаются согласованными.

6. Метрики оценки результативности внедрения СУИБ

1) Количество успешно завершенных попыток резервного копирования критичной информации, хранящейся на АРМ сотрудников, должно быть не менее 90%.

2) Количество успешно отраженных вирусных атак должно быть на уровне 95% от общего объема атак.

3) Уровень осведомленности пользователей оценивается путем проведения регулярных тестирований по информационной безопасности. Результаты тестирования тщательно анализируются, проходной балл составляет 85% от общего объема вопросов.

4) Количество вовремя отраженных инцидентов ИБ должно находиться на уровне 90%.

7. Порядок пересмотра

Настоящая Методика подлежит пересмотру не реже одного раза в год либо в случае изменения факторов, влияющих на ее содержание.

Ответственный за ИБ

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Приложение 3

Утверждаю
Директор КОМПАНИИ
ФИО
_____
"___" _____ 20___ г

№ _____

Программа тестирования плана обеспечения непрерывности бизнеса в КОМПАНИИ

№	Название проверки	Описание проверки	Документ	Ответственный	Дата	Примечание
1.	**Первоначальное тестирование**	Проверка наличия и доступности документации: • список оповещения; • телефонный справочник; • политика резервного копирования; • структурная схема ЛВС; • перечни оборудования и ПО; • реестр информационных ресурсов; • контактная информация поставщиков оборудования и ПО; • сервисные контракты;	План обеспечения непрерывности бизнеса	Ответственный за ИБ Системный администратор	Июль 2014 г.	

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

№	Название проверки	Описание проверки	Документ	Ответственный	Дата	Примечание
		• инструкции по эксплуатации оборудования и средств связи.				
2.	**Восстановление файлов и баз данных**	Проверка восстановления следующих файлов и баз данных с резервных копий в соответствии с установленной процедурой резервного копирования: • восстановление конфигураций рабочих мест; • восстановление данных пользователей. Проверка восстановления данных с физических носителей, хранящихся/ находящихся в офисе компании. Контроль полноты и целостности восстановленных данных.	План обеспечения непрерывности бизнеса	Ответственный за ИБ Системный администратор	Июль 2014 г.	
3.	**Проверка работоспособности каналов связи**	Проверка работоспособности резервных каналов связи. Проверка пропускной способности резервных каналов связи.	План обеспечения непрерывности бизнеса	Ответственный за ИБ Системный администратор	Июль 2014г.	

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

№	Название проверки	Описание проверки	Документ	Ответственный	Дата	Примечание
		Проверка доступности каналов связи для приложений.				
4.	**Учебная аварийная ситуация**	Проверка действий персонала по списку оповещения. Проверка действий персонала при пожаре. Проверка действий персонала в случае аварии электроснабжения. Проверка действий персонала в случае затопления.	Аварийные процедуры	Руководитель аварийного планирования Ответственный за ИБ Системный администратор	Июль 2014 г.	

Ответственный за ИБ

Системный администратор

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

Приложение 4

Утверждаю
Директор КОМПАНИИ
ФИО
_____
"___" _____ 20___ г

Процедура управления корректирующими и превентивными мерами в области информационной безопасности

Регистрационный номер документа
Версия
Дата вступления в силу
Подготовлен

Место хранения документа в электронном виде

Москва
20__

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

История изменений

Дата	Версия	Автор изменений	Описание изменений

1. Термины и определения

Ответственный за ИБ (или администратор ИБ) – назначаемый руководством КОМПАНИИ (далее – компания) сотрудник, отвечающий за безопасное функционирование определенных информационных систем компании.

Информационная безопасность (далее – ИБ) – состояние максимальной защищенности информационной системы компании с минимальным ущербом для ее производительности и доступности.

Корпоративная информационная система (далее – КИС) – автоматизированная система компании, представляющая собой организационно упорядоченную совокупность данных (массивов документов), технических и программных средств, технологий, реализующих информационные процессы.

Корректирующая мера – процесс реагирования на существующие проблемы ИБ и их исправление.

Несоответствие – нарушение требований ИБ, предъявляемых компанией.

Превентивная мера – процесс обнаружения потенциальных проблем ИБ и их устранение.

Риск ИБ – предполагаемое событие в области информационной безопасности, способное нанести ущерб компании и/или ее клиентам.

Система ИБ – совокупность защитных мер, средств и процессов их эксплуатации, направленных на достижение состояния защищенности информационных ресурсов.

Система управления информационной безопасностью (СУИБ) – это часть общей системы управления, основанная на оценке бизнес-рисков, которая предназначена для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования информационной безопасности.

Угроза ИБ – возможность реализации воздействия на информацию, обрабатываемую в КИС, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты КИС, приводящего к утрате, уничтожению или сбою функционирования носителя информации, средства взаимодействия с носителем или средства его управления.

2. Цель корректирующих и превентивных мер

Корректирующие и превентивные меры предназначены для:

1) устранения причин нарушения требований ИБ компании;
2) профилактики инцидентов информационной безопасности;
3) минимизации рисков ИБ;

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

4) устранения потенциальных угроз ИБ;
5) снижения и оптимизации стоимости поддержки системы ИБ;
6) непрерывного совершенствования СУИБ;
7) оперативного реагирования на изменение условий функционирования КИС компании.

3. Перекрестные документы

- Международный стандарт ISO 27001
- Политика системы управления информационной безопасностью
- План обеспечения непрерывности бизнеса
- Процедура проведения внутреннего аудита информационной безопасности

4. Полномочия и ответственность

Управление корректирующими и превентивными мерами осуществляется администратором ИБ.

В рамках реализации Процедуры управления корректирующими и превентивными мерами (далее – Процедура) администратор ИБ уполномочен привлекать к реализации мер профильных специалистов компании, обладающих экспертной подготовкой в предметной области принимаемых корректирующих или превентивных мер.

За ненадлежащее исполнение настоящей Процедуры штатные и внештатные сотрудники компании несут ответственность в соответствии с законодательством РФ и внутренними нормативными документами компании.

5. Процедура управления корректирующими и превентивными мерами

Порядок применения корректирующих и превентивных мер включает в себя:

1. Получение аналитической информации (данные аудиторских проверок, данные журналов событий, экспертные заключения в области ИБ, данные из иных публичных источников);
2. Сопоставление аналитической информации с требованиями ИБ;
3. Проведение анализа необходимости реализации корректирующих действий на основе утвержденных в компании критериев оценки эффективности мер безопасности;
4. Разработка Плана корректирующих или превентивных мер с указанием причины возникновения несоответствия (например, по результатам аудита);
5. Применение корректирующих или превентивных мер.

Причина возникновения несоответствий может быть указана в заголовке плана корректирующих действий.

На этапе получения аналитической информации осуществляется сбор данных, свидетельствующих о существовании несоответствий или неучтенных в СУИБ рисков.

В ходе сопоставления собранной аналитической информации о несоответствиях устанавливаются расхождения с принятыми в компании требованиями ИБ и принимается решение о необходимости применения корректирующих или превентивных мер.

Реализация плана корректирующих или превентивных мер заключается в определении действий, процедур, механизмов, направленных на устранение выявленных несоответствий, рисков и причин их возникновения.

105082, Россия, г. Москва
ул. Большая Почтовая, 55/59с
Телефон: +7 (495) 972-98-26
E-mail: info@it-task.ru

6. Периодичность проведения работ

Сотрудник, ответственный за ИБ, не реже одного раза в год проводит анализ процедуры управления корректирующими и превентивными мерами, а также оценку принятых корректирующих и превентивных мер с целью определения их эффективности.

7. Пересмотр и внесение изменений

Правила должны пересматриваться в случае существенных изменений в процедуре управления корректирующими и превентивными мерами, но не реже одного раза в год.

Ответственность за своевременный пересмотр и внесение изменений в Правила возлагается на сотрудника, ответственного за ИБ.

Ответственный за ИБ