**Состав исходной информации для оценки системы менеджмента**

**В.9. Состав исходной информации для оценки системы менеджмента информационной безопасности организаций на соответствие требованиям СТБ ISО 27001-2016 в любой области деятельности**

**В.9.1** Сведения об организации:

**В.9.1.1** Наименование организации

**В.9.1.2** Юридический адрес и фактический адрес

**В.9.1.3** Телефон, факс, адрес электронной почты, сайт

**В.9.1.4** Банковские реквизиты

**В.9.1.5** ФИО руководителя организации

**В.9.1.6** ФИО, телефон, факс, адрес электронной почты представителя руководства

**В.9.1.7** Отрасль промышленности

**В.9.1.8** Наименование консалтинговой организации, время оказания консалтинга

**В.9.1.9** Перечень поставщиков информационных услуг и услуг по информационной безопасности, переданных сторонним организациям (аутсорсинг):

|  |  |
| --- | --- |
| Процесс и поставщик | Описание процесса переданного на аутсорсинг |
|  |  |

**В.9.2.** Организационная структура и персонал

**В.9.2.1** Структурная схема организации, включающая основные и вспомогательные производственные подразделения, инженерные и административные службы с указанием связей между ними;

**В.9.2.2** Схема управления СМИБ (органиграмма) с идентификацией местонахождения подразделения (должностного лица), обеспечивающего функционирование системы менеджмента информационной безопасности;

**В.9.2.3** Количество сотрудников

|  |  |
| --- | --- |
|  Адрес или  обозначение площадкиПодразделение | Количество персонала по производственным площадкам и количество автоматизированных рабочих мест |
| Название площадки | Название площадки | … | … | … |
| Администрация |  |  |  |  |  |
| Конструкторские службы |  |  |  |  |  |
| Производственные подразделения |  |  |  |  |  |
|  Из них: разработчики собственного программного обеспечения |  |  |  |  |  |
| Отделы продаж, маркетинга, логистики  |  |  |  |  |  |
| IT-подразделения |  |  |  |  |  |
| Подразделения контроля качества |  |  |  |  |  |
| Прочие подразделения  |  |  |  |  |  |
| Всего человек в организации |  |  |  |  |  |
| Технические характеристики площадок |
| Общее количество настольных и мобильных компьютеров; (центральный офис/площадка); |  |  |  |  |  |
| Число физических серверов (центральный офис/площадка) |  |  |  |  |  |
| Общее количество коммуникационных узлов(маршрутизаторы, коммутаторы) (центральный офис/площадка); |  |  |  |  |  |
| Наличие поддерживаемых зон безопасности (центральный офис/площадка); |  |  |  |  |  |
| Использование защищенных каналов передачи данных, таких как VPN и др. (центральный офис/площадка); |  |  |  |  |  |
| Наличие Других параметров, характеризующих информационную среду организации или ее технические характеристики для расчета трудоемкости проведения аудита (центральный офис/площадка); |  |  |  |  |  |

**В.9.2.4** Существенные изменения в организационной структуре предприятия, документации СМИБ, влияющие на целостность СМИБ (при повторной сертификации).

**В.9.2.5** Общая численность персонала организации.

**В.9.2.6** Численность работающих, на которых распространяется область действия системы менеджмента информационной безопасности (в том числе; занимающегося разработкой, производством, обслуживанием, контролем, поставкой продукции, менеджментом информационной безопасности, материально-техническим снабжением; административно-управленческий аппарат).

**В.9.2.7** Средняя загруженность временных сотрудников;

**В.9.2.8** Стандартные часы работы организации;

**В.9.2.9** Количество сотрудников, которые работают за пределами площадки;

**В.9.2.10** Сменность работ на основном производстве (количество рабочих смен);

**В.9.2.11** Наличие и количество производственного персонала с неполной занятостью и (или) привлекаемого по договору.

**В.9.3** Сведения о филиалах:

- количество филиалов всего/ из них входит в область сертификации/ количество филиалов, объединенных одинаковой производственной деятельностью;

- юридическое лице (одно или несколько);

- численность персонала без учета работающих в филиалах (центральный офис);

-в филиалах используются методы и процедуры одни и те же или разные

- СМИБ в филиалах управляется централизовано/ не централизовано (основные критерии управления: управление документацией, программа внутреннего аудита, анализ со стороны руководства, управление претензиями потребителей, работа с жалобами, инцидентами, предписаниями контролирующих органов, различными законодательными требованиями, оценка корректирующих и предупреждающих действий).

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование и адрес филиала, ответственный представитель | Численность персонала, количество смен | Виды деятельности, виды продукции | Право заключения контрактов, есть/нет |
|  |  |  |  |

**В.9.4** Информационная структура организации:

**В.9.4.1** Законодательные требования (наименования лицензии, сертификатов, разрешений, деклараций, заключений, внешних нормативных документов, регламентирующих вопросы информационной безопасности организации);

**В.9.4.2** Применяемые в организации международные, межгосударственные, и национальные стандарты, отраслевые требования к информационной безопасности.

**В.9.4.3** Применяемые в организации рекомендации компаний-производителей программного и аппаратного обеспечения (Microsoft, Oracle, Cisco и др.)

**В.9.4.4** Применяемое в организации компьютерное программное обеспечение (собственной разработки или приобретенное), используемое в производимой организацией продукции (если это имеет место). Количество IT – платформ, количество операционных систем, количество процессов, связанных с информационной безопасностью, переданных на аутсорсинг.

**В.9.4.5.** Использование в организации общественных телекоммуникационных сетей (Интернета) для сбора, хранения и передачи данных (если используется, то какого рода информация обрабатывается).

**В.9.5** Используемое в организации программное обеспечение и активы

| **Тип программного обеспечения** | Наличие (да/нет) | **Описание использования** |
| --- | --- | --- |
| Системное ПО |  |  |
| Программные средства защиты: |
| [Криптошлюзы](http://ru.wikipedia.org/w/index.php?title=%D0%9A%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D1%88%D0%BB%D1%8E%D0%B7%D1%8B&action=edit) |  |  |
| [Средства аутентификации](http://ru.wikipedia.org/w/index.php?title=%D0%A1%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%D0%B0_%D0%B0%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D0%B8&action=edit) |  |  |
| [Средства мониторинга и аудита](http://ru.wikipedia.org/w/index.php?title=%D0%A1%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%D0%B0_%D0%BC%D0%BE%D0%BD%D0%B8%D1%82%D0%BE%D1%80%D0%B8%D0%BD%D0%B3%D0%B0_%D0%B8_%D0%B0%D1%83%D0%B4%D0%B8%D1%82%D0%B0&action=edit) |  |  |
| [Сканеры защищенности](http://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%BA%D0%B0%D0%BD%D0%B5%D1%80%D1%8B_%D0%B7%D0%B0%D1%89%D0%B8%D1%89%D0%B5%D0%BD%D0%BD%D0%BE%D1%81%D1%82%D0%B8&action=edit) |  |  |
| [Средства разграничения доступа](http://ru.wikipedia.org/w/index.php?title=%D0%A1%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%D0%B0_%D1%80%D0%B0%D0%B7%D0%B3%D1%80%D0%B0%D0%BD%D0%B8%D1%87%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0&action=edit) |  |  |
| [Системы криптографической защиты, шифрования и ЭЦП](http://ru.wikipedia.org/w/index.php?title=%D0%A1%D0%B8%D1%81%D1%82%D0%B5%D0%BC%D1%8B_%D0%BA%D1%80%D0%B8%D0%BF%D1%82%D0%BE%D0%B3%D1%80%D0%B0%D1%84%D0%B8%D1%87%D0%B5%D1%81%D0%BA%D0%BE%D0%B9_%D0%B7%D0%B0%D1%89%D0%B8%D1%82%D1%8B%2C_%D1%88%D0%B8%D1%25%20) |  |  |
| [Антивирусные программы](http://ru.wikipedia.org/wiki/%D0%90%D0%BD%D1%82%D0%B8%D0%B2%D0%B8%D1%80%D1%83%D1%81%D0%BD%D1%8B%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B) |  |  |
| [Антиспамовые программы](http://ru.wikipedia.org/w/index.php?title=%D0%90%D0%BD%D1%82%D0%B8%D1%81%D0%BF%D0%B0%D0%BC%D0%BE%D0%B2%D1%8B%D0%B5_%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D1%8B&action=edit) |  |  |
| [Межсетевой экран](http://ru.wikipedia.org/wiki/%D0%9C%D0%B5%D0%B6%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9_%D1%8D%D0%BA%D1%80%D0%B0%D0%BD) |  |  |
| Инструментальное ПО: |
| Средства разработки программного обеспечения  |  |  |
| [Системы управления базами данных](http://ru.wikipedia.org/wiki/%D0%A1%D0%A3%D0%91%D0%94) (СУБД)  |  |  |
| Прикладное ПО: |
| [Офисные приложения](http://ru.wikipedia.org/w/index.php?title=%D0%9E%D1%84%D0%B8%D1%81%D0%BD%D1%8B%D0%B5_%D0%BF%D1%80%D0%B8%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%B8%D1%8F&action=edit)  |  |  |
| [Корпоративные информационные системы](http://ru.wikipedia.org/w/index.php?title=%D0%9A%D0%BE%D1%80%D0%BF%D0%BE%D1%80%D0%B0%D1%82%D0%B8%D0%B2%D0%BD%D1%8B%D0%B5_%D0%B8%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86%D0%B8%D0%BE%D0%BD%D0%BD%D1%8B%D0%B5_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC%25D%20)  |  |  |
| Системы проектирования и производства  |  |  |
| Системы логистической поддержки изделий  |  |  |
| Научное ПО  |  |  |
| Телематика, передача данных, телефонное ПО, хостинг |  |  |
| Клиенты для доступа к интернет-сервисам |  |  |
| [Мультимедиа](http://ru.wikipedia.org/wiki/%D0%9C%D1%83%D0%BB%D1%8C%D1%82%D0%B8%D0%BC%D0%B5%D0%B4%D0%B8%D0%B0)  |  |  |
| Прочие системы |  |  |

**В.9.6** Заявление о политике и целях в области информационной безопасности, процедуры и средства управления, поддерживающие СМИБ, описания методологии оценки риска, отчет по оценке риска, план обработки риска, документированные процедуры, необходимые организации для обеспечения результативности планирования, функционирования и управления процессами ИБ, положение о применимости.

**В.9.7** Результаты внутренних аудитов (программы и обобщенные отчеты по внутренним аудитам) и записи.

**В.9.8** Отчет по анализу системы менеджмента качества со стороны руководства и решения по результатам анализа.

**В.9.9** Сведения о проверках органами Государственного надзора:

- последний акт проверки;

- планы корректирующих мероприятий;

- отчеты о выполнении корректирующих мероприятий.

**В.9.10** Результаты устранения несоответствий и выполнения аспектов для улучшения, выявленных при предыдущем аудите (при повторной сертификации).

**В.9.11** Применение сертификата соответствия и знака соответствия (при повторной сертификации).

**В.9.12** Наличие улучшений в СМИБ (при повторной сертификации).

Руководитель организации \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_