Анкета-вопросник

для проведения сертификации системы менеджмента информационной безопасности

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*наименование организации-заявителя*

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

*область применения СМИБ, применительно к которой осуществляются работы по сертификации*

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Самооценка соответствия требованиям к СМИБ** | | |
|  | Наименование вопроса | Заполняет организация | |
| Документ, в котором описана  процедура | |
| **1** | **2** | | **3** |
|  | **4.1 Понимание организации и ее контекста** | |  |
| 1 | Определены ли внешние и внутренние факторы, которые значимы с точки зрения ее целей и оказывают воздействие на способность достигать намеченных результатов ее системы менеджмента информационной безопасности? | |  |
|  | **4.2 Понимание потребностей и ожиданий заинтересованных сторон** | |  |
| 2 | Определены ли в организации  a) заинтересованные стороны, которые имеют отношение к системе менеджмента информационной  безопасности;  b) требования этих заинтересованных сторон, которые относятся к информационной безопасности? | |  |
|  | **4.3 Определение области применения СМИБ** | |  |
| 3 | Определены ли в организации границы и применимость СМИБ ? | |  |
| 4 | Рассмотрены ли при определении области применения:  a) внешние и внутренние факторы; указанные в п. 4.1?  b) требования, указанные в п. 4.2;  c) взаимосвязи и зависимости между деятельностью, выполняемой организацией, и деятельностью других организаций? | |  |
| 5 | Доступна и поддерживается ли область применения в виде документированной информации? | |  |
|  | **4.4 СМИБ** | |  |
| 6 | Разработана, внедрена, поддерживается ли СМИБ в соответствии с требованиями СТБ ISO/IEC 27001-2016? Проводится ли постоянное улучшение СМИБ? | |  |
|  | **5.1Лидерство и приверженность** | |  |
| 7 | Высшее руководство демонстрирует лидерство и приверженность по отношению к СМИБ посредством:  a) обеспечения того, чтобы для СМИБ были установлены политика информационной безопасности и цели информационной безопасности и чтобы они были согласованы со стратегическим направлением организации;  b) обеспечения интеграции требований СМИБ в процессы организации;  c) обеспечения того, чтобы ресурсы, необходимые для СМИБ, были доступны;  d) доведения до сведения важности результативного менеджмента информационной безопасности и соответствия требованиям СМИБ;  e) обеспечения того, чтобы СМИБ достигала своих намеченных результатов;  f) направления и поддержки персонала, который вносит вклад в результативность СМИБ;  g) содействия постоянному улучшению; и  h) поддержки других соответствующих ролей менеджеров для демонстрации ими лидерства применительно к областям их обязанностей? | |  |
|  | **5.2 Политика** | |  |
| 8 | Установлена ли высшим руководством политика информационной безопасности, которая:  a) соответствует назначению организации;  b) включает цели информационной безопасности или является основой для установления целей информационной безопасности;  c) включает обязательства соответствовать применимым требованиям, относящимся к информационной безопасности;  d) включает обязательство постоянно улучшать систему менеджмента информационной безопасности?  Политика информационной :  е) доступна и поддерживается в виде документированной информации?  f) доведена до сведения внутри организации?  g) доступна заинтересованным сторонам? | |  |
|  | **5.3 Роли, обязанности и полномочия в организации** | |  |
| 9 | Обеспечивается ли высшим руководством, чтобы обязанности и полномочия в отношении соответствующих ролей, имеющих отношение к информационной безопасности, назначались и доводились до сведения?  Назначены ли обязанности и полномочия для обеспечения соответствия СМИБ стандарту?  Назначены ли обязанности и полномочия для предоставления отчетов о пригодности СМИБ для высшего руководства? | |  |
|  | **6 Планирование**  **6.1.1 Действия по рассмотрению рисков и возможностей** | |  |
| 10 | Рассмотрены ли факторы и требования, определены ли риски и возможности для того, чтобы: гарантировать, что СМИБ может достигать намеченных результатов; предупредить или снизить нежелательные последствия; достичь улучшения?  Организация планирует действия по рассмотрению этих рисков и возможностей?  Организация планирует интегрировать и внедрять эти действия в процессы СМИБ?  Организация планирует оценивать результативность этих действий? | |  |
|  | **6.1.2 Оценка риска информационной безопасности** | |  |
| 11 | Организация определила и применяет ли процесс оценки риска информационной безопасности, который:  a) устанавливает и поддерживает критерии риска информационной безопасности, которые включают:  1) критерии принятия риска;  2) критерии для осуществления оценок риска информационной безопасности;  b) обеспечивает, что повторные оценки риска информационной безопасности позволят получить логичные, обоснованные и сопоставимые результаты;  c) обеспечивает идентификацию рисков информационной безопасности:  1) включает процесс оценки риска информационной безопасности, направленный на идентификацию рисков, связанных с потерей конфиденциальности, целостности и доступности информации в рамках области применения системы менеджмента информационной безопасности;  2) идентифицирует владельцев рисков;  d) обеспечивает анализ рисков информационной безопасности:  1) оценку потенциальных последствий, которые могут возникнуть в случае реализации рисков, указанных в 6.1.2, перечисление с), позиция 1);  2) оценку вероятности возникновения рисков, указанных в 6.1.2, перечисление с), позиция 1);  3) определение уровней риска;  e) обеспечивает оценку рисков информационной безопасности:  1) сравнение результатов анализа рисков с критериями рисков, установленными в 6.1.2, перечисление  а);  2) расстановку рисков по приоритетам для последующей обработки рисков?  Сохраняется ли документированная информация о процессе оценки рисков информационной безопасности? | |  |
|  | **6.1.3 Обработка рисков информационной безопасности** | |  |
| 12 | Организация определила и применяет ли процесс обработки риска информационной безопасности?  Сохраняется ли документированная информация о процессе обработки риска информационной безопасности? | |  |
|  | **6.2 Цели информационной безопасности и планирование их достижения** | |  |
| 13 | Организация установила цели информационной безопасности для соответствующих функций и уровней? | |  |
| 14 | Цели информационной безопасности:  - согласованы с политикой информационной безопасности?  - измеримы?  - учитывают применимые требования информационной безопасности, а также результаты оценки и обработки рисков?  - доводятся до сведения?  - обновляются при необходимости? | |  |
| 15 | Организация поддерживает документированную информацию о целях информационной безопасности? | |
| 16 | Для достижения целей организация определила:  - что будет сделано?  - какие ресурсы потребуются?  - кто будет ответственным?  - когда это будет завершено?  - каким образом будут оцениваться результаты? | |
|  | **7. Поддержка**  **7.1 Ресурсы** | |  |
| 17 | Определены ли и предоставляются ли ресурсы, необходимые для разработки, внедрения, поддержания и постоянного улучшения системы менеджмента информационной безопасности? | |  |
|  | **7.2 Компетентность** | |  |
| 18 | Организация определила необходимую компетентность персонала, осуществляющего работу под ее управлением, которая воздействует на пригодность и результативность информационной безопасности? | |  |
| 19 | Организация обеспечила, чтобы этот персонал обладал компетентностью на основе соответствующего образования, подготовки или опыта? | |  |
| 20 | Осуществлялись ли действия по приобретению необходимой компетентности и оценивалась ли результативность предпринятых действий? | |  |
| 21 | Сохранялась ли соответствующая документированная информация как свидетельство компетентности? | |  |
|  | **7.3 Осведомленность** | |  |
| 22 | Обеспечивает ли организация, чтобы соответствующий персонал, работающий под управлением организации, был :  - о политике информационной безопасности;  - его вкладе в результативность СМИБ, включая выгоды от улучшения пригодности информационной безопасности;  - последствиях несоответствий требованиям СМИБ? | |  |
|  | **7.4 Коммуникации** | |  |
| 23 | Организация определила внутренние и внешние коммуникации, относящиеся к СМИБ, включая:  - о чем будут осуществляться коммуникации;  - когда будут осуществляться коммуникации;  - с кем будут осуществляться коммуникации;  - кто будет осуществлять коммуникации;  - процессы, посредством которых должны осуществляться коммуникации? | |  |
|  | **7.5 Документированная информация** | |  |
| 24 | Включает ли система менеджмента информационной безопасности организации:  a) документированную информацию, требуемую настоящим стандартом;  b) документированную информацию, определенную организацией как необходимую для результативности системы менеджмента информационной безопасности? | |  |
|  | **7.5.2 Создание и обновление** | |  |
| 25 | Обеспечивается ли при создании и обновлении документированной информации:  a) идентификацию и описание (например, наименование, дата, автор или учетный номер);  b) формат (например, язык, версия программного обеспечения, графика) и носитель (например, бумажный, электронный);  c) анализ и одобрение сточки зрения приемлемости и адекватности? | |  |
|  | **7.5.3 Управление документированной информацией** | |  |
| 26 | Документированная информация, требуемая СМИБ находится под управлением?  Обеспечивается ли доступность и приемлемость для использования, где и когда это необходимо?  Документированная информация адекватна защищена (например, от нарушения конфиденциальности, ненадлежащего использования или нарушения целостности)?  Для управления документированной информацией организация рассмотрела распределение, доступ восстановление и использование?  Накопление и обеспечение сохранности, включая сохранение разборчивости?  Управление изменениями (например, управление версиями)?  Хранение и размещение?  Документированная информация внешнего происхождения, определенная организацией как необходимая для планирования и функционирования СМИБ, идентифицирована и управляема? | |  |
|  | **8 Операционная деятельность** | |  |
|  | **8.1 Планирование и управление деятельностью** | |  |
| 27 | Обеспечено ли планирование, внедрение и управление процессами, необходимыми для выполнения требований информационной безопасности? | |  |
| 28 | Сохраняется ли документированная информация в объеме, необходимом для получения уверенности в том, что процессы выполнены так, как запланировано? | |  |
| 29 | Обеспечено ли управление запланированными изменениями и анализируются ли последствия непредполагаемых изменений, принимая при необходимости действия по смягчению любых неблагоприятных последствий? | |  |
| 30 | Обеспечивается ли, определение управление аутсорсинговыми процессами? | |  |
|  | **8.2 Оценка рисков информационной безопасности** | |  |
| 31 | Выполняется ли оценка рисков информационной безопасности с учетом критериев, установленных в 6.1.2 перечисление а), через запланированные интервалы времени, или когда предполагаются или произошли существенные изменения? | |  |
| 32 | Сохраняется ли документированная информация о результатах оценок риска информационной безопасности? | |  |
|  | **8.3 Обработка риска информационной безопасности** | |  |
| 33 | Выполняет ли организация план обработки риска информационной безопасности? | |  |
| 34 | Сохраняется ли документированная информация о результатах обработки риска информационной безопасности? | |  |
|  | **9 Оценивание пригодности** | |  |
|  | **9.1 Мониторинг, измерения, анализ и оценивание** | |  |
| 35 | Проводит ли организация оценивание пригодности информационной безопасности и результативности системы менеджмента информационной безопасности? | |  |
| 36 | Определила ли организация:  a) что должно быть объектом мониторинга и измерений, в том числе процессы информационной безопасности и средства управления;  b) методы мониторинга, измерения, анализа и оценивания, насколько это применимо для обеспечения валидированных результатов;  c) когда должны выполняться мониторинг и измерения;  d) кто должен осуществлять мониторинг и измерения;  e) когда результаты мониторинга и измерений должны быть проанализированы и оценены;  f) кто должен анализировать и оценивать эти результаты?. | |  |
| 37 | Сохраняется ли документированная информация о результатах мониторинга и измерений? | |  |
|  | **9.2 Внутренний аудит** | |  |
| 38 | Проводит ли организация внутренние аудиты через запланированные интервалы времени для предоставления информации о том, что СМИБ соответствует требованиям организации к своей СМИБ и стандарту, а так же, что СМИБ результативно внедрена и поддерживается? | |  |
| 39 | Организация планирует, устанавливает, выполняет и поддерживает программу аудита, которая включает частоту, методы, обязанности, планируемые требования и отчетность и которая должна принимать во внимание важность процессов и результаты предыдущих аудитов?  Организация определяет для каждого аудита критерии и область применения аудита?  Организация отбирает аудиторов и проводит аудит так, чтобы была обеспечена объективность и беспристрастность процесса аудита?  Организация обеспечивает, чтобы результаты аудитов были доведены до сведения соответствующего руководства? | |  |
| 40 | Организация сохраняет программу аудита и результаты аудитов как документированную информацию? | |  |
|  | **9.3 Анализ со стороны руководства** | |  |
| 41 | Проводится ли высшим руководством анализ системы менеджмента информационной безопасности организации через запланированные интервалы времени для обеспечения ее постоянной приемлемости, адекватности и результативности? | |  |
| 42 | Включает ли анализ со стороны руководства следующее:  a) статус действий, проводимых по результатам предыдущих анализов со стороны руководства;  b) изменения в соответствующих внешних и внутренних факторах, касающихся системы менеджмента информационной безопасности;  c) обратную связь о текущем состоянии информационной безопасности, включая тенденции в:  1) несоответствиях и корректирующих действиях;  2) результатах мониторинга и измерений;  3) результатах аудитов;  4) результатах достижения целей информационной безопасности;  d) обратную связь от заинтересованных сторон;  е) результаты оценки рисков и статус выполнения плана обработки рисков; и  f) возможности для постоянного улучшения? | |  |
| 43 | Включают ли выходы анализа со стороны руководства решения и действия, связанные с реализацией возможностей для постоянного улучшения и любыми потребностями в изменениях системы менеджмента информационной безопасности?  Сохраняет ли организация результаты анализа со стороны руководства как документированную информацию? | |  |
|  | **10 Улучшение**  **10.1 Несоответствия и корректирующие действия** | |  |
| 44 | Если возникает несоответствие организация предпринимает действия, направленные на то, чтобы:  a) отреагировать на несоответствие и, если применимо:  1) предпринять действия по его управлению и коррекции;  2) бороться с последствиями;  b) оценить необходимость действий по устранению причины (причин) несоответствия с тем, чтобы оно не повторилось или не возникло в другом месте, посредством:  1) анализа несоответствия;  2) определения причин несоответствия;  3) определения того, что существуют ли аналогичные несоответствия или могут ли они потенциально возникнуть;  c) выполнить все необходимые действия;  d) проанализировать результативность каждого выполненного корректирующего действия;  e) при необходимости внести изменения в систему менеджмента информационной безопасности?  Обеспечено ли соответствие корректирующих действий последствиям выявленных несоответствий? | |  |
| 45 | Сохраняет ли организация документированную информацию как свидетельство:  f) характера несоответствий и всех последующих предпринятых действий;  д) результатов каждого корректирующего действия? | |  |
| 46 | Организация постоянно повышает приемлемости, адекватности и результативности СМИБ? | |  |

**Перечислить политики информационной безопасности, которые определяют средства управления согласно приложению А СТБ ISO/IEC 27001-2016:**

1.

2.

*Составил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (должность, ФИО, дата, подпись)*

