# АНКЕТА-ВОПРОСНИК

# для самооценки организации по требованиям ISO/IEC 27001:2022

**АНКЕТА-ВОПРОСНИК**

Для проведения самооценки просим Вас заполнить эту анкету, подписать её и вернуть в БелГИСС. Запрещается копировать анкету без разрешения БелГИСС.

|  |
| --- |
| Требования:ISO/IEC 27001:2022 |

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

наименование организации

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

область применения СМИБ, применительно к которой осуществляются работы по сертификации системы менеджмента информационной безопасности

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

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

Ф.И.О., должность лица, ответственного за систему менеджмента информационной безопасности организации, служебный тел.

Дата заполнения анкеты: «\_\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 20\_\_\_ г. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 подпись

Пояснения по заполнению: в графе «Обозначение документа» приводится ссылка на документ, содержащий подтверждение выполнения требования.

Таблица 1

| ПунктISO/IEC 27001 | Вопрос | Обозначение документа  | Комментарии |
| --- | --- | --- | --- |
| 4.1 | Определен ли контекст организации, включая 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 а) | Определены ли в организацииa) заинтересованные стороны, которые имеют отношение к системе менеджмента информационнойбезопасности; |  |  |
| 4.2 b) | b) требования этих заинтересованных сторон, которые относятся к информационной безопасности?Включают ли они законодательные, нормативные требования и договорные обязательства? |  |  |
| 4.2 c) | Определены ли в организацииc) требования этих заинтересованных сторон, которые относятся к информационной безопасности?Включают ли они законодательные, нормативные требования и договорные обязательства? |  |  |
| 4.3 | Определены ли в организации границы и применимость системы менеджмента информационной безопасности, чтобы установить область ее применения? |  |  |
| 4.3 | Рассмотрены ли при определении области применения:a) внешние и внутренние факторы, указанные в 4.1;b) требования, указанные в 4.2;c) взаимосвязи и зависимости между деятельностью, выполняемой организацией, и деятельностьюдругих организаций? |  |  |
| 4.3 | Поддерживается ли область применения в виде документированной информации? |  |  |
| 4.4 | Разработана и внедрена ли документально оформленная СМИБ в соответствии с требованиями ISO/IEC 27001-2022Поддерживается ли документально оформленная СМИБ в рабочем состоянии?Проводится ли постоянное улучшение СМИБ? |  |  |
| 5.1 | Демонстрирует ли высшее руководство должно лидерство и приверженность по отношению ксистеме менеджмента информационной безопасности посредством:a) обеспечения того, чтобы для системы менеджмента информационной безопасности былиустановлены политика информационной безопасности и цели информационной безопасности и чтобыони были согласованы со стратегическим направлением организации;b) обеспечения интеграции требований системы менеджмента информационной безопасностив процессы организации;c) обеспечения того, чтобы ресурсы, необходимые для системы менеджмента информационнойбезопасности, были доступны;d) доведения до сведения важности результативного менеджмента информационной безопасностии соответствия требованиям системы менеджмента информационной безопасности;e) обеспечения того, чтобы система менеджмента информационной безопасности достигаласвоих намеченных результатов;f) направления и поддержки персонала, который вносит вклад в результативность системы менеджментаинформационной безопасности;д) содействия постоянному улучшению; иh) поддержки других соответствующих ролей менеджеров для демонстрации ими лидерства применительно к областям их обязанностей? |  |  |
| 5.2  | 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? |  |  |
| 5.2  | Обеспечивается ли чтобы Политика информационной безопасности:е) поддерживалась в виде документированной информации;f) доводилась до сведения внутри организации;д) была доступной, при необходимости, соответствующим заинтересованным сторонам? |  |  |
| 5.3 | Обеспечено ли высшим руководством, чтобы обязанности и полномочия в отношении соответствующихролей, имеющих отношение к информационной безопасности, назначались и доводились до сведения. |  |  |
| 5.3 | Назначены ли высшим руководством обязанности и полномочия для:a) обеспечения того, чтобы система менеджмента информационной безопасности соответствовалатребованиям настоящего стандарта;b) предоставления отчетов о пригодности системы менеджмента информационной безопасностивысшему руководству? |  |  |
| 6.1.1 | Обеспечено ли при планировании системы менеджмента информационной безопасности организация рассмотрение факторов, приведенных в 4.1, и требований, приведенных в 4.2? |  |  |
| 6.1.1 | Определены ли риски и возможности, которые необходимы, чтобы:a) гарантировать, что система менеджмента информационной безопасности может достигатьнамеченных результатов;b) предупредить или снизить нежелательные последствия; иc) достичь постоянного улучшения? |  |  |
| 6.1.1 | Планируются ли:d) действия по рассмотрению этих рисков и возможностей; и то, как:1) интегрировать и внедрять эти действия в процессы системы менеджмента информационнойбезопасности;2) оценивать результативность этих действий? |  |  |
| 6.1.2  | Определен и применяется ли процесс оценки риска информационной безопасности,который:a) устанавливает и поддерживает критерии риска информационной безопасности, которые включают:1) критерии принятия риска; и2) критерии для осуществления оценок риска информационной безопасности;b) обеспечивает, что повторные оценки риска информационной безопасности позволят получитьлогичные, обоснованные и сопоставимые результаты;c) обеспечивает идентификацию рисков информационной безопасности:1) включает процесс оценки риска информационной безопасности, направленный на идентификациюрисков, связанных с потерей конфиденциальности, целостности и доступности информациив рамках области применения системы менеджмента информационной безопасности; и2) 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); и2) 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, перечислениеа); и2) расстановку рисков по приоритетам для последующей обработки рисков? Сохраняется ли документированная информация о процессе обработки риска информационной безопасности? |  |  |
| 6.1.3  | Определен ли и применяется ли процесс обработки риска информационной безопасности для: a) выбора соответствующих вариантов обработки рисков информационной безопасности с учетом результатов оценки риска; b) определения всех средств управления, которые необходимы для реализации выбранного варианта (ов) обработки риска информационной безопасности.c) сравнения средств управления, определенных в 6.1.3, перечисление b), с приведенными вПриложении A, для удостоверения того, что не были упущены необходимые средства управления; d) разработки положения о применимости, которое содержит необходимые средства управления (см. 6.1.3, перечисления b) и c)) и обоснования их включения (независимо от того, внедрены ли они или нет), а также обоснования исключений средств управления из приложения A; e) разработки плана обработки рисков информационной безопасности; и f) получения одобрения плана обработки рисков информационной безопасности от владельцев рисков и подтверждения ими принятия остаточных рисков информационной безопасности?Сохраняется ли организацией документированная информация о процессе обработки риска информационной безопасности?  |  |  |
| 6.2  | Установлены ли цели информационной безопасности для соответствующих функций и уровней? |  |  |
| 6.2  | Обеспечивается ли чтобы цели информационной безопасности:a) были согласованны с политикой информационной безопасности;b) были измеримыми (если это применимо);c) учитывали применимые требования информационной безопасности, а также результаты оценки и обработки рисков;d) анализировались на выполнимость;e) доводились до сведения; иf) обновлялись при необходимости;g) поддерживаются ли в виде документированной информации? |  |  |
| 6.2  | Определено ли при планировании достижения своих целей информационной безопасности:a) что будет сделано;b) какие ресурсы потребуются;c) кто будет ответственным;d) когда это будет завершено; иe) каким образом будут оцениваться результаты? |  |  |
| 7.1  | Определены ли и предоставляются ли ресурсы, необходимые для разработки, внедрения, поддержания и постоянного улучшения системы менеджмента информационной безопасности? |  |  |
| 7.2  | Обеспечивается ли чтобы в организации:a) была определена необходимая компетентность персонала, осуществляющего работу под ее управлением, которая воздействует на пригодность информационной безопасности;b) обеспечивается, чтобы этот персонал обладал компетентностью на основе соответствующего образования, подготовки или опыта;c) если применимо, осуществляются ли действия по приобретению необходимой компетентности и оценивается ли результативность предпринятых действий? |  |  |
| 7.2  | Сохраняется ли соответствующая документированная информация как свидетельство компетентности. |  |  |
| 7.3  | Осведомлен ли персонал, работающий под управлением организации о:a) политике информационной безопасности;b) его вкладе в результативность системы менеджмента информационной безопасности, включаявыгоды от улучшения пригодности информационной безопасности; иc) последствиях несоответствий требованиям системы менеджмента информационной безопасности? |  |  |
| 7.4  | Определены ли внутренние и внешние коммуникации, относящиеся к системе менеджмента информационной безопасности, включая то:a) о чем будут осуществляться коммуникации;b) когда будут осуществляться коммуникации;c) с кем будут осуществляться коммуникации;d) кто должен осуществлять коммуникации;e) процессы, посредством которых должны осуществляться коммуникации? |  |  |
| 7.5.1  | 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  | 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  | Находится ли документированная информация, требуемая системой менеджмента информационной безопасности и стандартом, под управлением для обеспечения того, что она:a) доступна и приемлема для использования, где и когда это необходимо;b) адекватно защищена (например, от нарушения конфиденциальности, ненадлежащего использованияили нарушения целостности)? |  |  |
| 7.5.3  | Обеспечивается ли для управления документированной информацией рассмотрение следующей деятельности:c) распределение, доступ, восстановление и использование;d) накопление и обеспечение сохранности, включая сохранение разборчивости;e) управление изменениями (например, управление версиями); иf) хранение и размещение? |  |  |
| 7.5.3  | Определена ли как необходимая документированная информация внешнего происхождения, для планирования и функционирования системы менеджмента информационной безопасности? |  |  |
| 7.5.3  | Обеспечена ли идентификация и управление необходимой документированной информацией внешнего происхождения? |  |  |
| 8.1  | Обеспечено ли планирование, внедрение и управление процессами, необходимыми для выполнениятребований информационной безопасности? |  |  |
| 8.1  | Выполняются ли действия, по рассмотрению рисков и возможностей посредством: - установления критериев для процессов;- осуществления управления этими процессами в соответствии с установленными критериями? |  |  |
| 8.1  | Сохраняется ли документированная информация в объеме, необходимом для получения уверенности в том, что процессы выполнены так, как запланировано? |  |  |
| 8.1  | Обеспечено ли управление запланированными изменениями и анализируются ли последствия непредполагаемых изменений, принимая при необходимости действия по смягчению любых неблагоприятных последствий? |  |  |
| 8.1  | Обеспечивается ли, что переданные на выполнения на сторону процессы и предоставляемые извне продукция и услуги, имеющие значение для системы менеджмента информационной безопасности, находятся под управлением организации? |  |  |
| 8.2  | 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? |  |  |
| 8.2  | Сохраняется ли документированная информация о результатах оценок риска информационной безопасности? |  |  |
| 8.3 | Выполняется ли план обработки рисков информационной безопасности? |  |  |
| 8.3 | Сохраняется ли информация о результатах обработки риска информационной безопасности в виде документированной информации? |  |  |
| 9.1  | Проводится ли оценивание пригодности информационной безопасности и результативности системы менеджмента информационной безопасности? |  |  |
| 9.1  | Определено ли: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? |  |  |
| 9.1  | Сохраняется ли документированная информация о результатах мониторинга и измерений? |  |  |
| 9.1 | Оцениваются ли показатели информационной безопасности и результативность СМИБ? |  |  |
| 9.2.1 | Проводятся ли внутренние аудиты через запланированные интервалы времени для предоставления информации о том, что система менеджмента информационной безопасности:a) соответствует:1) требованиям организации к своей системе менеджмента информационной безопасности;2) требованиям настоящего стандарта;b) результативно внедрена и поддерживается? |  |  |
| 9.2.2 | Планируется, разрабатывается, выполнятся и поддерживается ли программу (ы) аудита, включая частоту, методы, обязанности, планируемые требования и отчетность? Принимается ли во внимание при разработке программ (ы) аудита важность процессов и результаты предыдущих аудитов?Обеспечила ли организация выполнение следующих требований:a) определять для каждого аудита критерии и область применения аудита;b) отбирать аудиторов и проводить аудит так, чтобы была обеспечена объективность и беспристрастность процесса аудита;c) обеспечивать, чтобы результаты аудитов были доведены до сведения руководства соответствующегоуровня? |  |  |
| 9.2.2  | Обеспечивается ли сохранение программы аудита и результатов аудитов как документированной информации? |  |  |
| 9.3.1 | Проводится ли высшим руководством анализ системы менеджмента информационной безопасности организации через запланированные интервалы времени для обеспечения ее постоянной приемлемости, адекватности и результативности? |  |  |
| 9.3.2 | 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 менеджментаинформационной безопасности;c) изменения в потребностях и ожиданиях заинтересованных сторон, имеющих значение для системы менеджмента информационной безопасности;d)информацию о функционировании СМИБ, включая тенденции в:1) несоответствиях и корректирующих действиях;2) результатах мониторинга и измерений;3) результатах аудитов;4) результатах достижения целей информационной безопасности;e) обратную связь от заинтересованных сторон;f) результаты оценки рисков и статус выполнения плана обработки рисков; g) возможности для постоянного улучшения? |  |  |
| 9.3.3 | Выходы анализа со стороны руководства должны включать решения и действия, связанные с реализацией возможностей для постоянного улучшения и любыми потребностями в изменениях системыменеджмента информационной безопасности.Организация должна сохранять результаты анализа со стороны руководства как документированную информацию. |  |  |
| 9.3  | Сохраняются ли результаты анализа со стороны руководства как документированная информация? |  |  |
| 10.1  | Обеспечивается ли деятельность, направленная на постоянное улучшение приемлемости, адекватности и результативности системы менеджмента информационной безопасности? |  |  |
| 10.2 | Обеспечивается ли при выявлении несоответствия 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, чтобыоно не повторилось или не возникло в другом месте, посредством:1) анализа несоответствия;2) определения причин несоответствия; и3) определения того, что существуют ли аналогичные несоответствия или могут ли они потенциальновозникнуть;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? |  |  |
| 10.2 | Обеспечивается ли сохранение документированной информации как свидетельство:f) характера несоответствий и всех последующих предпринятых действий;g) результатов каждого корректирующего действия? |  |  |

**Требования приложения А ISO/IEC 27001:2022**

Таблица 2

| Требование приложения А ISO/IEC 27001:2022 | **Средство управления\*** |
| --- | --- |
| 1. Организационные средства управления
 |
| 5.1 | Политики информационной безопасности |  |
| 5.2 | Роли и ответственность в областиинформационной безопасности |  |
| 5.3 | Разделение обязанностей |  |
| 5.4 | Обязанности, ответственность руководства |  |
| 5.5 | Взаимодействие с уполномоченными органами |  |
| 5.6 | Взаимодействие с профессиональными сообществами |  |
| 5.7 | Исключение угроз |  |
| 5.8 | Информационная безопасность в управлении проектами |  |
| 5.9 | Инвентаризация информации и связанных с ней активов |  |
| 5.10 | Надлежащее применение информационных и иных, связанных с ними, активов |  |
| 5.11 | Возврат активов |  |
| 5.12 | Классификация информации |  |
| 5.13 | Маркировка информации |  |
| 5.14 | Передача информации |  |
| 5.15 | Управление доступом |  |
| 5.16 | Управление идентификацией |  |
| 5.17 | Информация для аутентификации |  |
| 5.18 | Права доступа |  |
| 5.19 | Информационная безопасность в отношениях с поставщиками |  |
| 5.20 | Обеспечение информационной безопасности в рамках соглашений с поставщиками |  |
| 5.21 | Управление информационной безопасностью в цепочках поставки в сфере ИКТ |  |
| 5.22 | Мониторинг, анализ и управление изменениями услуг поставщиков |  |
| 5.23 | Информационная безопасность при использовании облачных сервисов |  |
| 5.24 | Планирование и подготовка в области управления инцидентами информационной безопасности |  |
| 5.25 | Оценка событий в области информационной безопасности и принятие решений |  |
| 5.26 | Реагирование на инциденты информационной безопасности |  |
| 5.27 | Извлечение уроков из инцидентов информационной безопасности |  |
| 5.28 | Сбор свидетельств |  |
| 5.29 | Информационная безопасность при сбое |  |
| 5.30 | Готовность ИКТ к обеспечению непрерывности бизнеса |  |
| 5.31 | Законодательные, нормативные и договорные требования |  |
| 5.32 | Права интеллектуальной собственности |  |
| 5.33 | Защита записей |  |
| 5.34 | Конфиденциальность и защита персональных данных |  |
| 5.35 | Независимый анализ информационной безопасности |  |
| 5.36 | Соответствие политикам, правилам и стандартам информационной безопасности |  |
| 5.37 | Документированные операционные процедуры |  |
| **6 Средства управления, связанные с персоналом** |
| 6.1 | Предварительная проверка  |  |
| 6.2 | Условия трудового соглашения |  |
| 6.3 | Осведомленность, образование и подготовка в сфере информационной безопасности |  |
| 6.4 | Дисциплинарные меры |  |
| 6.5 | Обязанности после прекращения или изменения трудовых отношений |  |
| 6.6 | Соглашения о конфиденциальности или неразглашении |  |
| 6.7 | Удаленная работа |  |
| 6.8 | Отчетность о событиях информационной безопасности |  |
| 7 Средства управления, связанные с физическим доступом |
| 7.1 | Физические периметры безопасности |  |
| 7.2 | Физический вход |  |
| 7.3 | Защита офисов, помещений и устройств |  |
| 7.4 | Мониторинг физической защиты |  |
| 7.5 | Защита от физических и природных угроз |  |
| 7.6 | Работа в защищенных зонах |  |
| 7.7 | Чистый стол и чистый экран |  |
| 7.8 | Размещение и защита оборудования |  |
| 7.9 | Защита активов вне территории |  |
| 7.10 | Устройства хранения |  |
| 7.11 | Службы обеспечения |  |
| 7.12 | Защита кабельных сетей |  |
| 7.13 | Обслуживание оборудования |  |
| 7.14 | Безопасная утилизация или повторное использование оборудования |  |
| 8 Технологические средства управления |
| 8.1 | Конечные устройства пользователя |  |
| 8.2 | Привилегированные права доступа |  |
| 8.3 | Ограничения доступа к информации |  |
| 8.4 | Доступ к исходному коду |  |
| 8.5 | Безопасная аутентификация |  |
| 8.6 | Управление производительностью |  |
| 8.7 | Защита от вредоносного программного обеспечения |  |
| 8.8 | Управление техническими уязвимостями |  |
| 8.9 | Менеджмент конфигураций |  |
| 8.10 | Удаление информации |  |
| 8.11 | Шифрование данных |  |
| 8.12 | Предупреждение утечки данных |  |
| 8.13 | Резервное копирование информации |  |
| 8.14 | Избыточность устройств обработки информации |  |
| 8.15 | Ведение журналов (логов) |  |
| 8.16 | Мониторинг действий |  |
| 8.17 | Синхронизация часов |  |
| 8.18 | Использование утилит с привилегированными правами |  |
| 8.19 | Установка приложений в операционной системе |  |
| 8.20 | Безопасность сетей |  |
| 8.21 | Безопасность сетевых сервисов |  |
| 8.22 | Разделение сетей |  |
| 8.23 | Веб-фильтрация |  |
| 8.24 | Использование криптографии |  |
| 8.25 | Жизненный цикл разработки безопасного программного обеспечения |  |
| 8.26 | Применение требований по безопасности |  |
| 8.27 | Безопасная архитектура систем и принципы разработки |  |
| 8.28 | Безопасное кодирование |  |
| 8.29 | Тестирование обеспечения безопасности при разработке и приемке |  |
| 8.30 | Разработка, переданная на аутсорсинг |  |
| 8.31 | Разделение среды разработки, тестирования и эксплуатации |  |
| 8.32 | Управление изменениями |  |
| 8.33 | Данные для тестирования |  |
| 8.34 | Защита информационных систем в ходе аудита |  |