
**Ассоциация пользователей стандартов по информационной
безопасности «АБИСС»**

**СТАНДАРТ
ОРГАНИЗАЦИИ**

**СТО
7721490330-001–
2023**

УТВЕРЖДАЮ

Председатель АБИСС


А.А. Харыбина



**Оказание услуг по оценке соответствия требованиям информационной
безопасности
Общие требования и порядок оказания услуг.**

**Москва
2023**

Предисловие

1 РАЗРАБОТАН Ассоциация пользователей стандартов по информационной безопасности «АБИСС»

2 УТВЕРЖДЕН Ассоциация пользователей стандартов по информационной безопасности «АБИСС»

3 ВВЕДЕН ВПЕРВЫЕ

Правила применения настоящего стандарта организации установлены в статье 21 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Текст настоящего стандарта организации размещается в информационной системе общего пользования – на официальном сайте Ассоциацией пользователей стандартов по информационной безопасности «АБИСС» (Ассоциация «АБИСС»).

СТАНДАРТ ОРГАНИЗАЦИИ

Оказание услуг по оценке соответствия требованиям информационной безопасности Общие требования

Provision of services for assessing compliance with information security requirements
General requirements

1. Область применения

Настоящий стандарт устанавливает общие требования по оказанию услуг по оценке соответствия требованиям информационной безопасности в целях формирования и систематизации лучших практик по проведению оценок соответствия по требованиям информационной безопасности.

Настоящий стандарт применяется представителями проверяемых и проверяющих организаций при планировании и проведении внешних аудитов (оценок соответствия) на соответствие требованиям информационной безопасности.

Настоящий стандарт позволит проверяющим организациям построить и повысить уровень зрелости процесса проведения оценок соответствия. Настоящий стандарт позволит проверяемым организациям повысить качество проводимых оценок соответствия путем формирования требований к проверяющим организациям и процессу проведения оценок соответствия.

2. Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организациях. Основные термины и определения

ГОСТ Р 57580.1-2017 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер"

ГОСТ Р 57580.2-2018 "Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Методика оценки соответствия"

ГОСТ Р 57580.3-2022 "Безопасность финансовых (банковских) операций. Управление риском реализации информационных угроз и обеспечение операционной надежности. Общие положения"

ГОСТ Р 57580.4-2022 "Безопасность финансовых (банковских) операций. Обеспечение операционной надежности. Базовый состав организационных и технических мер"

ГОСТ Р ИСО/МЭК 15408-3-2013 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности"

ГОСТ Р 59547-2021 "Защита информации. Мониторинг информационной безопасности. Общие положения"

ГОСТ Р 59709-2022 "Защита информации. Управление компьютерными инцидентами. Термины и определения"

ГОСТ Р 59710-2022 "Защита информации. Управление компьютерными инцидентами. Общие положения"

ГОСТ Р 59711-2022 "Защита информации. Управление компьютерными инцидентами. Организация деятельности по управлению компьютерными инцидентами"

ГОСТ Р 59712-2022 "Защита информации. Управление компьютерными инцидентами. Руководство по реагированию на компьютерные инциденты"

Примечание – При использовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования – на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3. Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 57580.1 – 2017, ГОСТ 5780.2-2018, ГОСТ Р 53114-2008, в том числе следующие термины:

3.1 информационная безопасность организации (ИБ организации): Состояние защищенности интересов организации в условиях угроз в информационной сфере.

Примечание - Защищенность достигается обеспечением совокупности свойств информационной безопасности - конфиденциальностью, целостностью, доступностью информационных активов и инфраструктуры организации. Приоритетность свойств информационной безопасности определяется значимостью информационных активов для интересов (целей) организации.

3.2 оценка соответствия (аудит) требованиям информационной безопасности: Процесс оценки выбора и реализации организацией организационных и технических мер защиты информации в соответствии с установленными требованиями, выполняемый проверяющей организацией.

3.3 свидетельство аудита информационной безопасности (свидетельство): Записи, изложение фактов или другая информация, которые имеют отношение к критериям аудита информационной безопасности организации и могут быть проверены.

Примечание — Свидетельства аудита могут быть качественными или количественными.

3.4 проверяющая организация: Организация, проводящая оценку соответствия (аудит) требованиям информационной безопасности и являющаяся независимой от проверяемой организации.

3.4 проверяющая группа: Группа, состоящая из сотрудников проверяющей организации, а также (при необходимости) иных лиц, уполномоченных проверяющей организацией участвовать в оценке соответствия (аудите) требованиям информационной безопасности проверяемой организации.

3.5 проверяемая организация: Организация, в отношении которой проводится оценка соответствия (аудит) требованиям информационной безопасности.

4. Требования к проверяющей организации

4.1. Деловая репутация и лицензируемая деятельность

4.1.1. Проверяющая организация не должна находиться в реестре недобросовестных поставщиков, а также у нее не должно быть признаков предбанкротного состояния и конкурсного производства.

4.1.2. Проверяющая организация должна обладать лицензиями и сертификатами, необходимыми для проведения оценки соответствия:

- лицензия на проведение работ и услуг, предусмотренных подпунктами "б", "д" или "е" пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации [1];
- лицензии и сертификаты, требуемые регулятором или системой сертификации.

4.1.3. Проверяющая организация должна иметь сертификат Системы добровольной сертификации АБИСС на оказание услуг по проведению оценок соответствия требованиям национальных стандартов.

4.2. Отсутствие конфликта интересов

4.2.1. Проверяющая и проверяемая организации не должны быть аффилированы. К этому можно относить:

- нахождение организаций под управлением одних лиц;
- включение организаций в одну группу компаний или функционирование в качестве дочерней организации;
- любые прочие факторы, указывающие на связь между организациями или лицами, ими управляющими.

4.2.2. В проверяемой организации не должны работать представители проверяющей организации.

4.2.3. В проверяющей организации должна быть утверждена "Политика по управлению конфликтом интересов", отражающая подходы организации по обеспечению объективной и независимой оценки.

4.2.3.1. В Политике должны быть определены и зафиксированы процедуры проверки аффилированности и зависимости между проверяемой и проверяющей организациями.

4.2.3.2. В Политике должны быть определены и зафиксированы направления деятельности, состав работ и услуг, из-за которых может возникнуть конфликт интересов в проверяющей организации при выполнении оценок соответствия, а также указаны способы снижения конфликта интересов.

4.2.3.3. В Политике должен быть отражен запрет на включение в рекомендации после завершения оценки соответствия ИТ/ИБ решений, продуктов и услуг, реализуемых проверяющей организацией, без предложения альтернатив (при их наличии).

4.2.3.4. В Политике должна быть отражена процедура формирования проверяющей группы, которая, в том числе, ограничивает включение в проверяющую группу работников, которые на период проверки и за последние два года до начала проверки участвовали в оказании иных, кроме проверки, ИТ/ИБ услуг проверяемой организации.

4.2.3.5. В Политике должны быть отражены процедуры контроля обеспечения независимости участников проверяющей группы при оказании других услуг, помимо аудита

информационной безопасности или оценки соответствия, проверяемой организации со стороны проверяющей.

4.2.3.6. Политика должна содержать требование о необходимости включения в отчет о результатах оценки соответствия всех фактов, которые могут вызвать конфликт интересов, а также информации о том, как обеспечивается его недопущение.

4.2.3.7. Политика должна содержать требование по ознакомлению с данной Политикой всех работников организации, участвующих в оценках соответствия, обязательство по ее выполнению и ответственность организации и работника за нарушение Политики.

4.3. Достаточность ресурсов

4.3.1. В проверяющей организации должна быть утверждена “Политика по управлению ресурсами”, отражающая подходы организации в управлении временными и кадровыми ресурсами для целей проведения оценок соответствия.

4.3.2. В Политике должны быть определены ограничения по одновременному участию сотрудников в проектах.

4.3.3. В Политике должен быть отражен процесс сквозного управления ресурсами для принятия решения о выделении ресурсов на новый проект.

4.3.4. В Политике должна быть описана процедура выделения ресурсов на проект:

4.3.4.1. Перед началом оценки соответствия должен оцениваться необходимый объем ресурсов для проекта в соответствии с методикой оценки ресурсов, утвержденной в проверяющей организации.

4.3.4.2. Методика оценки ресурсов для проекта должна оценивать объективные критерии о предстоящей оценке соответствия, в том числе: набор национальных стандартов и НПД для проведения оценки, направления деятельности организации, технологические процессы, инфраструктуру организации, размер и значимость организации.

4.3.4.3. Результат оценки ресурсов на проект должен определять минимально необходимые значения для количества участников проверяющей группы, минимальную квалификацию участников проверяющей группы, минимально необходимую длительность оценки соответствия.

4.3.5. Требования по минимально необходимому ресурсному обеспечению для проекта определяются «Политикой по управлению ресурсами» и/или методиками проведения оценки соответствия.

4.4. Компетентность и обеспечение повышения профессиональных навыков работников

4.4.1. В проверяющей организации должна быть утверждена “Политика по повышению профессиональных навыков работников”, регламентирующая:

- процесс планирования систематического повышения профессиональных навыков работников.
- процесс согласования и выделения ресурсов на повышение профессиональных навыков работников.
- процесс проверки профессиональных навыков работников.
- требования к способам повышения навыков работников, например: обучение в аккредитованных образовательных учреждениях, прохождение курсов разработчиков и вендоров технических систем, изучение материалов и публикаций профессиональных

сообществ, обучение по зарекомендовавшим себя базам знаний и лучшим практикам, отработка практических навыков на тестовых площадках, развернутых в инфраструктуре организации.

- требования к управлению собственной базой знаний.
- требования к хранению документов, свидетельствующих о повышении профессиональных навыков работниками, а также регламент предоставления этих свидетельств, в том числе, по запросу проверяемой организации.

4.5. Контроль качества

4.5.1. В проверяющей организации должна быть утверждена «Политика по контролю качества», которая определяет принципы, процедуры и ответственность за обеспечение качества услуг по оценке соответствия требованиям информационной безопасности.

4.5.2. Политика должна распространяться на все этапы и процессы, связанные с проведением оценок соответствия требованиям информационной безопасности, осуществляемых проверяющей организацией.

4.5.3. Политика должна описывать процедуры по контролю качества, включая:

4.5.3.1. Внутренний аудит – регулярные проверки на соответствие внутренним стандартам и требованиям регуляторов процессов оказания услуг по оценке соответствия.

4.5.3.2. Верификация отчетов – независимый пересмотр специалистом, не принимавшим участие в проведении оценки соответствия, результатов оценки перед их передачей проверяемой организации.

4.5.3.3. Получение обратной связи от проверяемых организаций – сбор и анализ отзывов для улучшения качества услуги по оценке соответствия.

4.5.4. Политика должна описывать процессы оценки эффективности и улучшения процедур контроля качества, включая периодичность проведения оценки эффективности, анализ результатов контроля качества и внесение изменений.

4.5.5. Политика должна описывать зоны ответственности при обеспечении качества оказываемых услуг по оценке соответствия, включая ответственность руководства компании, менеджера по качеству, руководителей и участников проверяющих групп.

4.6. Обеспечение конфиденциальности

4.6.1. В проверяющей организации должна быть утверждена «Политика по обеспечению конфиденциальности», которая включает в себя основные принципы работы с конфиденциальной информацией, классификацию информации с учетом уровней конфиденциальности, требования к мерам защиты и правила обработки информации при оказании услуг по оценке соответствия требованиям информационной безопасности.

4.6.2. Политика должна соответствовать законодательству Российской Федерации и национальным стандартам в области защиты конфиденциальной информации, включая защиту персональных данных.

4.6.3. В Политике должны быть отражены принципы обработки получаемой в рамках проведения оценки соответствия информации, включая:

- принцип законности - обработка только при наличии правового основания,
- принцип ограничения целей - сбор и использование только в установленных целях,

- принцип минимизации данных - сбор только необходимого объема информации.

4.6.4. В Политике должны быть описаны все виды получаемой проверяющей организацией конфиденциальной информации при проведении оценки соответствия, включая внутренние документы проверяемой организации, результаты наблюдений, выгрузки из информационных систем и другие свидетельства, а также результаты проведения оценки соответствия. Для каждого вида получаемой информации должен быть установлен уровень конфиденциальности.

4.6.5. В Политике должны быть описаны правила обработки конфиденциальной информации в зависимости от уровня конфиденциальности на всех этапах обработки, включая получение, регистрацию, хранение, использование, передачу, обезличивание и уничтожение информации.

4.6.6. В Политике должны быть описаны организационные и технические меры защиты, обеспечивающие конфиденциальность информации на всех этапах ее жизненного цикла, включая требования по шифрованию информации и разрешенные каналы ее передачи, а также правила защиты бумажных носителей.

4.6.7. В Политике должен быть описан порядок доступа сотрудников к конфиденциальной информации, основанный на принципе минимально необходимых привилегий, который устанавливает правила предоставления, изменения и прекращения прав доступа.

4.6.8. В Политике должны быть закреплены обязанности сотрудников по соблюдению конфиденциальности, включая обязательство подписать соглашение о неразглашении. Должна быть установлена персональная ответственность руководителей подразделений за соблюдение Политики их сотрудниками, а также виды дисциплинарной, материальной и иной ответственности за нарушение положений Политики.

4.6.9. В Политике должны быть определены этапы реагирования на утечки информации и установлены сроки и способы уведомления заинтересованных сторон.

4.7. Условия привлечения соисполнителей

4.7.1. При необходимости проверяющая организация по согласованию с проверяемой может привлечь соисполнителя к процессу оценки соответствия.

4.7.2. Ответственность за проведение работ и качество их выполнения, а также соблюдение требований ИБ и конфиденциальности соисполнителем в процессе проведения работ остается на головной проверяющей организации.

4.7.3. В качестве руководителя проверяющей группы может выступать только работник головной проверяющей организации.

4.7.4. В случае привлечения физического лица в качестве соисполнителя, оно должно соответствовать требованиям к проверяющим специалистам и не являться сотрудником проверяемой организации.

5. Требования к проверяющим специалистам

5.1. Квалификационные требования руководителя проверяющей группы

5.1.1. Наличие либо законченного высшего образования по направлению информационной безопасности, либо законченной программы профессиональной переподготовки по направлению информационной безопасности (не менее 512 часов).

5.1.2. Наличие подтвержденного опыта проведения оценок соответствия требованиям ИБ за последний год.

5.1.3. Наличие подтверждения квалификации аудитора по одному из международных стандартов в области ИБ или подтверждения прохождения обучения по российскому стандарту с удостоверением государственного образца.

5.1.4. Наличие сертификата Системы добровольной сертификации АБИСС, подтверждающего квалификацию по оценке соответствия требованиям национальных стандартов.

5.2. Квалификационные требования участника проверяющей группы

5.2.1. Наличие либо оконченого высшего образования по направлению информационной безопасности или подтверждения процесса его получения, либо оконченой программы профессиональной переподготовки по направлению информационной безопасности (не менее 512 часов), либо оконченого среднего специального образования по направлению информационной безопасности.

5.2.2. Наличие сертификата Системы добровольной сертификации АБИСС, подтверждающего квалификацию по оценке соответствия требованиям национальных стандартов.

6. Требования к планированию проведения оценки соответствия

6.1. Постановка целей

6.1.1. Цель оценки должна включать обязательство провести оценку соответствия качественно, с полным покрытием области оценки, с формированием объективных, обоснованных выводов и оценок.

6.1.2. Цель не должна быть определена в виде конечных количественных или качественных показателей оценки соответствия, имеющих заданные заранее значения.

6.2. Определение области оценки соответствия

6.2.1. Определение области оценки соответствия осуществляется проверяющей организацией и согласуется с проверяемой организацией до начала проведения оценки соответствия. В случае разногласия в определении области оценки проверяющая организация отражает факт разногласия в отчете в соответствующем разделе.

6.2.2. Область оценки соответствия должна учитывать организационную структуру проверяемой организации, ее географическое распределение, а также соответствовать области применения регулирующих нормативных актов в части объектов информатизации, технологических и бизнес-процессов.

6.3. Определение участников оценки соответствия

6.3.1. Заказчик проведения оценки соответствия

6.3.1.1. Проверяемая организация может не быть заказчиком проведения оценки соответствия. В этом случае проверяемая организация должна подтвердить свое согласие на проведение оценки соответствия до заключения договора.

6.3.1.2. Процедура согласования и эскалации должна предусматривать участие заказчика.

6.3.1.3. Договором должно быть определено, кому передается отчет с результатами проведения оценки соответствия.

6.3.2. Состав проверяющей и проверяемой группы

6.3.2.1. Со стороны проверяющей группы выделяются следующие роли, которые могут совмещаться:

- Координатор проверяющей группы: администрирует процессы оценки соответствия со стороны проверяющей организации, согласовывает с проверяемой стороной способы и форматы обмена данных, обеспечивает урегулирование конфликтов.
- Руководитель проверяющей группы (главный аудитор): утверждает план проведения оценки соответствия, распределяет задачи для участников проверяющей группы, принимает решение о выполнении\невыполнении конкретных мер и выставляемых оценок, утверждает отчет по оценке соответствия со стороны проверяющей группы.
- Участник проверяющей группы: проводит проверочные мероприятия и фиксирует его результаты, участвует в формировании отчета по оценке соответствия.

6.3.2.2. Со стороны проверяемой группы выделяются следующие роли, которые могут совмещаться:

- Координатор проверяемой организации: администрирует процессы оценки соответствия со стороны проверяемой организации, согласовывает с проверяющей стороной способы и форматы обмена данных, обеспечивает присутствие интервьюируемых при проведении оценки соответствия, обеспечивает предоставление сведений в согласованные сроки, консолидирует данные для предоставления проверяющей организации, обеспечивает урегулирование конфликтов;
- Участник проверяемой организации: предоставляет информацию в области своей ответственности, относящейся к оценке соответствия.

6.3.3. Изменения в составе участников

6.3.3.1. Изменения в состав проверяющей группы могут вноситься только по согласованию с проверяемой организацией. Все участники проверяющей группы должны соответствовать требованиям к проверяющим специалистам.

6.3.3.2. При смене координатора проверяемая организация должна уведомить проверяющую организацию и обеспечить передачу необходимых данных о ходе выполнения оценки соответствия новому координатору.

6.4. Выделение проверяемой организацией ресурсов для проведения оценки соответствия

6.4.1. До начала оценки соответствия проверяющей организации должен быть предоставлен Приказ о проведении оценки соответствия, подтверждающий выделение кадровых и временных ресурсов для интервью, сбора свидетельств и сопровождения проверяющих, а также подтверждающий предоставление контролируемого допуска представителям проверяющей организации для проведения проверочных мероприятий и сбора свидетельств.

6.4.2. Проверяющей организации должен быть предоставлен комплект организационно-распорядительных документов по информационной безопасности, действующий на момент оценки соответствия, а также комплект документов или реестров, описывающих объекты информационной инфраструктуры, а также технологические и бизнес-процессы организации.

6.5. Составление плана проведения оценки соответствия

6.5.1. План проведения оценки соответствия составляется проверяющей организацией и согласовывается с проверяемой организацией.

6.5.2. План проведения оценки соответствия должен быть выполнен и учитывать область оценки соответствия, используемые технологии, а также технологические и бизнес-процессы организации.

6.5.3. Внесение изменений в план в ходе проведения оценки соответствия согласовывается сторонами.

6.5.4. План должен отражать ход предстоящих работ, состав работ, сроки и результаты по ним. Рекомендуемый объем состава работ: определение состава рабочих групп, определение области оценки, сбор и анализ документации, проведение интервью и наблюдений, сбор свидетельств, проведение технических исследований, анализ собранных свидетельств, подготовка, согласование и утверждение отчета. Работы, выполняемые проверяющей организацией, могут идти параллельно. Необходимость определяется проверяющей организацией в зависимости от объема работ.

6.6. Выбор методов сбора свидетельств

6.6.1. Проверяющая организация определяет и согласовывает с проверяемой методы сбора свидетельств. Методы сбора свидетельств выбираются проверяющей организацией таким образом, чтобы обеспечить объективность и валидность выводов.

6.6.2. К методам сбора свидетельств относятся, в том числе, но не ограничиваясь: документальный анализ, интервью, визуальные наблюдения, а также анализ конфигураций и протоколов работы технических средств (прикладного ПО и ПАК, средств защиты информации), функционирующих в информационной структуре проверяемой организации. Использование проверяющей организацией иных технических средств для сбора свидетельств возможно при согласовании с проверяемой организацией.

6.7. Порядок взаимодействия в ходе проведения оценки соответствия

6.7.1. Между проверяющей и проверяемой группами должен быть согласован порядок взаимодействия, включая порядок передачи сведений, процедуру согласования отчета по результатам оценки соответствия, а также процедуру эскалации для каждой из сторон в случае необходимости.

6.7.2. Порядок взаимодействия должен, в частности, определять требования к обеспечению конфиденциальности, формату и способу передачи свидетельств, а также документообороту.

7. Требования к проведению оценки соответствия

7.1. Определение выборки из области оценки соответствия

7.1.1. Оценка соответствия может проводиться на основе выборки, которая определяется проверяющей организацией и обосновывается в отчете.

7.1.2. Выборку можно применять только для типовых и единообразных элементов области оценки соответствия.

7.1.3. Выборка не может применяться для технологических и бизнес-процессов, а также для технологических участков, в рамках которых реализуются технологические и/или бизнес-процессы. Выборка автоматизированных систем должна обеспечивать оценку соответствия для

каждого технологического и бизнес-процесса, попадающего в область оценки, а также для каждого технологического участка, в рамках которого реализуются эти технологические и/или бизнес-процессы.

7.1.4. Выборка должна быть релевантной и репрезентативной, достаточной для формирования выводов по всей области оценки.

7.1.5. Из выборки могут быть исключены внутренние структурные подразделения финансовой организации, в которых нет самостоятельных (независимых от централизованных) технологических и бизнес-процессов, а также технологических участков, в рамках которых реализуются данные технологические и/или бизнес-процессы.

7.1.6. Нельзя исключать из выборки элементы области оценки, которые находятся на аутсорсинге.

7.2. Сбор свидетельств

7.2.1. Состав и качество свидетельств

7.2.1.1. Проверяющей организацией должны быть запрошены и получены актуальные свидетельства в необходимом и достаточном объеме для формирования выводов о выполнении требований и реализации мер защиты.

7.2.1.2. Проверяющей организации необходимо обеспечить доступность, полноту собранных свидетельств в формате и качестве, позволяющим их впоследствии анализировать.

7.2.1.3. Собранные свидетельства не должны противоречить выводам. В случае, если полученные свидетельства имеют противоречивый характер, при формировании выводов применяется следующий подход к оценке достоверности свидетельств:

- преимущество отдается свидетельствам, полученным на основе анализа конфигурации и протоколов работы аппаратного и программного обеспечения, средств защиты информации, а также в ходе инструментальных проверок;
- в случае невозможности формирования выводов на основе указанных выше свидетельств, преимущество отдается:
 - свидетельствам, полученным в ходе непосредственного наблюдения за проверяемым процессом;
 - сведениям, содержащимся в учетных системах и контрольных записях по результатам выполнения требований (акты, протоколы, отчеты, журналы и т.д.);
 - обобщенным результатам опроса работников различного уровня, вовлеченных в проверяемый процесс;
 - документам, регламентирующим обследуемый процесс.

7.2.1.4. Проверяющей организацией должны быть запрошены и получены подтверждения выполнения требований с проверяемой организации в случаях, когда технологические процессы, объекты информационной инфраструктуры или меры защиты находятся на аутсорсинге.

7.2.2. Порядок сбора и фиксации свидетельств

7.2.2.1. Проверяющая организация должна вести учет запрошенных и собранных свидетельств в процессе оценки соответствия.

7.2.2.2. Проверяющая организация должна обеспечить хранение собранных свидетельств с момента начала проведения оценки соответствия в течение 5 лет после ее завершения.

7.2.3. Неотчуждаемые свидетельства

7.2.3.1. Если копии документов в бумажном виде не могут быть переданы проверяющей организации и методикой оценки не установлена обязательность их приложения к отчету, то в присутствии участника проверяющей группы эти документы должны быть учтены как отдельные единицы хранения. Реквизиты этих единиц хранения прикладываются к отчету в качестве отдельного свидетельства. При этом проверяемая организация берет на себя письменное обязательство обеспечить самостоятельное хранение учтенных документов. При утрате таких документов, перечень которых включен в отчет в качестве отдельного свидетельства, отчет становится недействителен.

7.2.3.2. Если документ в электронном виде не может быть передан проверяющей организации и методикой оценки не установлена обязательность их приложения к отчету, то в присутствии участника проверяющей группы работником проверяемой организации для каждого документа вычисляется хэш-функция, реализованная по ГОСТ Р 34.11 и организуется его хранение. Реквизиты документа и значение вычисленной для него хэш-функции прикладываются к отчету в качестве свидетельства. При этом проверяемая организация берет на себя письменное обязательство обеспечить самостоятельное хранение указанных свидетельств. При утрате таких свидетельств, или не совпадении хэш-функции хранимого документа с указанной в свидетельстве, отчет считается недействительным.

7.2.3.3. Если при полученные при наблюдении скриншоты или любые другие свидетельства наблюдения не могут быть переданы проверяющей организации и методикой оценки не установлена обязательность их приложения к отчету, то в присутствии участника проверяющей группы работником проверяемой организации для каждого файла, содержащего указанные свидетельства, вычисляется хэш-функция, реализованная по ГОСТ Р 34.11 и организуется его хранение. Реквизиты файла и значение вычисленной для него хэш-функции прикладываются к отчету в качестве свидетельства. При этом проверяемая организация берет на себя письменное обязательство обеспечить самостоятельное хранение указанных свидетельств. При утрате таких свидетельств, или не совпадении хэш-функции хранимого файла с указанной в свидетельстве, отчет считается недействительным.

7.2.4. Непредставление свидетельств

7.2.4.1. В случае непредставления свидетельств проверяющая организация вправе оценить требование как невыполненное.

7.2.4.2. В случае систематического непредставления свидетельств проверяющая организация должна поставить в известность контролирующие лица со стороны проверяемой организации согласно процедуре эскалации, определенной на этапе планирования, вплоть до направления официального письма на имя руководителя проверяемой организации.

7.2.4.3. В случае систематического непредставления свидетельств или существенного нарушения срока предоставления свидетельств при отсутствии реагирования на обращение проверяющей организации со стороны руководителя проверяемой организации дает право проверяемой организации завершить оценку с отрицательным результатом, включив в состав отчета указание на отказ проверяемой организации в предоставлении свидетельств.

7.2.5. Сбор свидетельств в случае аутсорсинга технологических процессов.

7.2.5.1. В случае, если компоненты инфраструктуры или процессы компании-аутсорсера попадают в область оценки или влияют на нее, должно быть получено подтверждение выполнения требований информационной безопасности:

- путем непосредственного включения инфраструктуры и процессов компании-аутсорсера в область оценки проверяемой организации и их обследования, что обеспечивается проверяемой организацией;
- путем представления документированных результатов (отчета) о проведении оценки соответствия инфраструктуры и процессов компании-аутсорсера с подтверждением, что процессы, входящие в область оценки проверяемой организации также были включены в область оценки компании-аутсорсера.

При этом оценка соответствия компании-аутсорсера в рамках данного процесса должна быть проведена в соответствии с требованиями данного стандарта, а также по требованиям действующих нормативно-правовых актов уровнем не ниже, чем к оценке соответствия проверяемой организации. При этом результаты оценки должны быть не ниже, чем минимально установленные требованиями для проверяемой организации. Результаты оценки соответствия должны содержать детальное описание процессов и услуг, включенных в область оценки, числовые или качественные результаты оценки, наименование организации, выполнившей проверку компании-аутсорсера.

Проверяющая организация может направить посредством проверяемой организации запрос компании-аутсорсеру на уточнение средств и способов выполнения требований в инфраструктуре, предоставляемой со стороны компании-аутсорсера проверяемой организации.

7.2.5.2. В случае непредставления подтверждения выполнения требований в случаях, когда технологические процессы, объекты информационной инфраструктуры или меры защиты находятся на аутсорсинге, проверяющая организация вправе оценить требования как невыполненные.

7.3. Подготовка отчета

7.3.1. Общие требования к отчету

7.3.1.1. Отчет должен быть представлен в бумажном и/или электронном виде в зависимости от используемой методики оценки. Электронный вид отчета должен иметь согласованный участниками формат.

7.3.1.2. Отчет должен включать всю требуемую информацию согласно выбранной методике оценки соответствия.

7.3.1.3. Собранные свидетельства являются неотъемлемой частью отчета.

7.3.1.4. Отчет должен содержать перечень приложений.

7.3.2. Требования к титульному листу и разделу со сводной информацией:

7.3.2.1. Титульный лист отчета должен содержать ID проекта по проведению оценки соответствия, присвоенный Системой добровольной сертификации АБИСС (СДС АБИСС), названия проверяемой и проверяющей организации, а также подписи сторон:

- со стороны проверяющей - руководитель организации, руководитель проверяющей группы;
- со стороны проверяемой - руководитель организации или уполномоченное лицо, ответственное за проведение оценки соответствия, координатор проверяемой группы.

7.3.2.2. Раздел со сводной информацией должен содержать:

- Сведения (названия) об участвующих сторонах, включая проверяемую и проверяющую организации, организацию заказчика, привлеченных соисполнителей, организаций-аутсорсеров и т.д.;

- Сроки проведения оценки соответствия и ее отдельных этапов: как фактические, так и определенные договором;
- Перечень регулирующих документов, на соответствие которым проводилась оценка соответствия;
- Перечень используемых методик оценки соответствия;
- Результат оценки соответствия согласно использованной методике;
- Наличие неразрешенных разногласий между проверяющей и проверяемой организацией;
- Наличие технологических процессов, объектов информационной инфраструктуры или мер защиты, переданных на аутсорсинг и входивших в область оценки соответствия;
- Отметка о конфиденциальном характере отчета и результатов оценки соответствия;
- Информация о согласии или несогласии с результатами отчета со стороны проверяемой организации;

7.3.3. Требования к разделу с информацией о сторонах

7.3.3.1. Отчет должен содержать сведения о заказчике проведения оценки соответствия:

- Сведения о заказчике (название, ОГРН, ИНН);
- Ответственный со стороны заказчика (ФИО, должность);
- Аффилированность заказчика и проверяемой организации, характер правовых отношений.

7.3.3.2. Отчет должен содержать сведения о проверяемой организации:

- Сведения о проверяемой организации (название, ОГРН, ИНН);
- Сведения об участниках проверяемой группы (ФИО, должность, роль);
- Сведения об изменениях в составе участников проверяемой организации в процессе проведения оценки соответствия, если они были.

7.3.3.3. Отчет должен содержать сведения о проверяющей организации:

- Сведения о проверяющей организации (название, ОГРН, ИНН, сертификат СДС АБИСС);
- Сведения о составе проверяющей группы на всех этапах оценки соответствия (ФИО, должность, роль, дата трудового договора, номер сертификата СДС АБИСС, подтвержденный опыт оценок соответствия для руководителя проверяющей группы);
- Сведения об изменениях в составе проверяющей группы в процессе проведения оценки соответствия, если они были;
- Сведения о возможном конфликте интересов, и предпринятые меры, обеспечивающие его недопущение.

7.3.3.4. Отчет должен содержать сведения о соисполнителях:

- Если в качестве участника проверяющей группы привлекается эксперт как физическое лицо, то информация о нем отражается в составе проверяющей группы и вместо трудового договора указывается номер и дата договора по оказанию его услуг, а также номер сертификата СДС АБИСС.
- Если в качестве соисполнителя привлекается организация, то в отчете указываются сведения об организации-соисполнителе (название организации, ОГРН, ИНН, номер сертификата СДС АБИСС), а также сведения об участвующих в оценке работниках организации-соисполнителя (ФИО, должность, роль, номер сертификата СДС АБИСС).

- В отчете указывается перечень и описание работ, для которых был привлечен каждый соисполнитель.

7.3.3.5. Отчет должен содержать сведения об организации-аутсорсере:

- Сведения об организациях, которым на аутсорсинг отданы технологические процессы, объекты информационной инфраструктуры или меры защиты (название, ОГРН, ИНН, лицензии для случаев аутсорсинга процессов ИБ);
- Сведения о переданных технологических процессах, объектах информационной инфраструктуры или мерах защиты – входили ли они в область оценки, было ли подтверждено соответствие в рамках проведенной оценки или по имеющимся у организации-аутсорсера результатам оценки соответствия.

7.3.4. Отчет должен содержать информацию об ИТ-инфраструктуре и топологии сети.

7.3.5. Отчет должен содержать информацию по области оценки и выборке.

7.3.5.1. Требования к описанию области оценки:

- В отчете должны быть перечислены элементы области оценки и их типы:
 - Технологические и бизнес-процессы, входящие в область оценки соответствия;
 - Автоматизированные системы и приложения, которые обеспечивают указанные выше технологические и бизнес-процессы, с указанием их назначения и соответствующим им процессов;
 - Типы объектов информатизации, на которые распространяется оценка соответствия. *Например: Linux и Windows серверы, АРМ, активное и пассивное сетевое оборудование, СУБД, системы виртуализации, СХД, терминалы оплаты;*
 - Типы территориальных объектов проверяемой организации, на которых расположены объекты информатизации, например: головной офис, дополнительный офис, филиал, ЦОД;
 - Роли сотрудников, которые участвуют в процессах или работают с объектами информатизации, которые попадают в область оценки соответствия;
- В отчете должны быть перечислены процессы, которые относятся к области применения, но которые не вошли в область оценки и приведено обоснование их исключения из области оценки.

7.3.5.2. Требования к описанию выборки из области оценки:

- В отчете должно быть приведено обоснование объема и состава выборки по типам элементов области оценки;
- В отчете должны быть перечислены и описаны вошедшие в выборку конкретные элементы области оценки со степенью детализации, позволяющей однозначно идентифицировать элемент в проверяемой организации; *Например: доменное имя сервера, адрес территориального объекта, ФИО и должность работника.*
- Для каждого элемента должно быть указано его назначение или роль.

7.3.6. В отчет рекомендуется включать информацию о ходе работы

- К отчету может быть приложен согласованный на этапе планирования план-график.
- К отчету может быть приложен фактический график работ.

7.3.7. Отчет должен содержать сведения о методике оценки соответствия

7.3.7.1. Перечень НПА и стандартов, на соответствие которым проводилась оценка соответствия.

7.3.7.2. Указание используемой методики проведения оценки соответствия. В случае, если используется собственная методика, то она должна быть описана в отчете.

7.3.7.3. Информация о выбранных методах проведения оценки соответствия (документальный анализ, интервью, использование технических средств для сбора свидетельств, визуальные наблюдения и т.д.).

7.3.8. Отчет должен содержать выводы о реализации мер.

7.3.8.1. Выводы о реализации меры должны быть основаны на собранных свидетельствах и не противоречить им.

7.3.8.2. Выводы о реализации меры должны быть аргументированы и описаны в таблице соотнесения оцениваемых мер и имеющихся свидетельств.

7.3.9. Отчет должен содержать итоги проведения оценки соответствия и рекомендации

7.3.9.1. Итоги оценки соответствия, содержащие следующую информацию:

- завершена ли оценка;
- достигнуты ли цели оценки;
- остались ли неразрешенные разногласия;
- итоговые числовые или качественные значения оценки и/или заключение о результате.

7.3.9.2. Краткое резюме для руководства проверяемой организации по результатам проверки с описанием результата, критичных нарушений и рисков по ним.

7.3.9.3. Рекомендации по повышению уровня соответствия. Рекомендации должны быть направлены на устранение нарушений и/или достижение необходимого уровня согласно методике.

7.3.10. Отчет должен содержать следующие реестры

7.3.10.1. Перечень неразрешенных разногласий между проверяющей группой и проверяемой организацией с указанием позиции каждой из сторон.

7.3.10.2. Перечень проведенных интервью.

7.3.10.3. Список электронных документов, хранящихся у проверяемой организации и их хэш-функции.

7.3.10.4. Список электронных файлов-свидетельств, хранящихся у проверяемой организации и их хэш-функции.

7.3.10.5. Список свидетельств на бумажном носителе, прикладываемых к отчету.

7.3.10.6. Список неотчуждаемых свидетельств на бумажном носителе, хранящихся у проверяемой организации и их с указанием их реквизитов учета.

7.3.10.7. Таблица соотнесения оцениваемых мер и имеющихся свидетельств.

8. Требования к завершению оценки соответствия

8.1. Согласование и доработка отчета

8.1.1. Процедура согласования должна быть определена на этапе планирования оценки соответствия.

8.1.2. Сроки согласования отчета должны быть определены в рамках договора.

8.2. Урегулирование разногласий участников

8.2.1. Процедура урегулирования должна быть определена на этапе планирования оценки соответствия.

8.2.2. Координаторы со стороны проверяемой и проверяющей организацией должны обеспечить процесс урегулирования разногласий на всех этапах оценки соответствия.

8.2.3. В случае если разногласия не могут быть урегулированы на уровне рабочих групп, то разногласие фиксируется с аргументированной позицией каждой из сторон и эскалируется на вышестоящего руководителя согласно процедуре урегулирования, согласованной на этапе планирования.

8.2.4. Если проверяемая организация не является заказчиком оценки соответствия, то разногласия эскалируются на заказчика.

8.2.5. Если для участия в оценке соответствия привлечен соисполнитель, то все разногласия решаются через головную проверяющую организацию.

8.2.6. При разрешении эскалированных разногласий составляется протокол урегулирования за подписью сторон в лице руководителей организаций или уполномоченных сотрудников. Протокол является неотъемлемой частью отчета.

8.2.7. В случае если разногласия не были урегулированы, составляется реестр всех неразрешенных разногласий между проверяющей группой и проверяемой организацией с указанием позиции каждой из сторон. Реестр подписывается руководителями проверяющей и проверяемой организаций или уполномоченными сотрудниками и является неотъемлемой частью отчета.

8.3. Утверждение и передача отчета

8.3.1. Проверяющая организация должна обеспечить контроль качества итогового отчета на предмет:

- полноты проведенной оценки соответствия и правильности определения и описания области оценки соответствия и выборке по ней;
- отсутствия противоречий и логических ошибок, а также достаточность обоснования выводов, приведенных в отчете;
- соответствия отчета используемым методикам оценки соответствия и внутренним требованиям проверяющей организации;
- корректности оформления и отсутствия грамматических и стилистических ошибок.

8.3.2. Отчет должен быть утвержден руководителем проверяющей организации.

8.3.3. Представитель проверяемой организации в отчете указывает, согласны ли участники рабочей группы от проверяемой организации с результатами отчета.

8.3.4. Отчет, включая собранные свидетельства, передается проверяемой организации в бумажном и/или электронном виде согласно методике оценке соответствия в защищенном виде. Отчет, включая собранные свидетельства, в электронном виде должен быть подписан УКЭП со стороны проверяющей организации.

8.4. Хранение отчета и передача третьим лицам

8.4.1. Проверяющая и проверяемая организации должны обеспечить хранение отчета вместе со свидетельствами в течение 5 лет после завершения оценки соответствия.

8.4.2. Если для выполнения работ были привлечены соисполнители, то соисполнители обязаны передать все собранные свидетельства проверяющей организации по акту приема-

передачи, после чего обязанность по хранению отчета и собранных свидетельств возлагается на головную проверяющую организацию. Соисполнители обязаны уничтожить хранящиеся у них свидетельства, обеспечив их конфиденциальность до момента уничтожения.

8.4.3. Проверяющая организация должна обеспечить конфиденциальность отчета.

Библиография

- [1] Постановление Правительства РФ от 3 февраля 2012 г. N 79 "О лицензировании деятельности по технической защите конфиденциальной информации" (с изменениями и дополнениями).

УДК 351.864.1:004:006.354

ОКС 03.060
35.240.40

Ключевые слова: оказание услуг по оценке соответствия требованиям информационной безопасности, оценка соответствия выполнения требований защиты информации
