

Реестр требований безопасности

написано Александр Астахов | 10 июня, 2023

Применимые к организации требования законодательной и нормативной базы, требования бизнеса, а также требования, вытекающие из контрактных обязательств организации, оформляются в виде реестра требований безопасности.

Идентификация требований безопасности:

- Идентифицируются:
 - законодательные и нормативные требования;
 - контрактные обязательства;
 - требования бизнеса.
- Цель:
 - идентификация юридических, репутационных, финансовых и бизнес-рисков, связанных с нарушением обязательных требований.

Реестр требований безопасности используется для оценки и контроля следующих рисков:

- юридических рисков, возникающих при нарушении организацией требований действующего законодательства и нормативной базы в области информационной безопасности;
- юридических, репутационных и финансовых рисков, связанных с невыполнением организацией контрактных

обязательств;

- бизнес-рисков, связанных с невыполнением требований бизнеса к обеспечению информационной безопасности, нарушение которых может повлечь причинение ущерба организации и затруднить достижение целей бизнеса.

Законодательные и нормативные требования

В данной таблице определяются требования действующего законодательства и нормативной базы в области информационной безопасности, применимые к Компании или ее деятельности, а также текущее состояние выполнения этих требований.

Краткая формулировка требования	Полная формулировка требования	Отметка о выполнении	Примечание
Федеральный закон Российской Федерации от 27 июля 2006 г. N 152-ФЗ "О персональных данных"			
1. Обеспечение конфиденциальности персональных данных всеми участниками процесса их обработки	Статья 6. Условия обработки персональных данных 4. В случае, если оператор на основании договора поручает обработку персональных данных другому лицу, существенным условием договора является обязанность обеспечения указанным лицом конфиденциальности персональных данных и безопасности персональных данных при их обработке. Статья 7. Конфиденциальность персональных данных 1. Операторами и третьими лицами, получающими доступ к персональным данным, должна обеспечиваться конфиденциальность таких данных	Y	
2. Получение письменного согласия на обработку персональных данных	Статья 6. Условия обработки персональных данных 1. Обработка персональных данных может осуществляться оператором с согласия субъектов персональных данных. Статья 7. Конфиденциальность персональных данных 4. В случаях, предусмотренных настоящим Федеральным законом,	Y	

Ответственность за формирование и поддержание в актуальном состоянии реестра требований информационной безопасности несет менеджер информационной безопасности. Актуализация и контроль выполнения требований осуществляется в ходе проведения плановых аудитов. При этом по каждому требованию в реестре проставляется отметка о выполнении, например, следующим образом:

- Y (Yes) – выполнено;
- QY (Quote Yes) – частично выполнено;
- N (No) – не выполнено;
- ? – проверка не проводилась.

В графе «Примечания» даются пояснения относительно выбранной отметки о выполнении/невыполнении требования.

Для каждого требования безопасности могут также указываться информационные активы, на которые это требование распространяется, и категория требования (конфиденциальность, целостность, доступность, аутентичность, неотказуемость).

Далее мы подробнее рассмотрим различные категории требований безопасности.