# ПРАВИЛА ПРОВЕДЕНИЯ ВНУТРЕННЕГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

**Астана**
**2023 г.**

## 1. Назначение и область применения

Настоящие Правила проведения внутреннего аудита информационной безопасности Информационной системы Организации (далее – Правила) разработаны в соответствии с требованиями разделов: 8.2.2 СТ РК ИСО 9001:2016, 6 СТ РК ИСО/МЭК 27001:2015.

1. Требования настоящих Правил распространяются на всех сотрудников ОЮЛ Ассоциация ВИЭ «Qazaq Green».
2. Настоящие Правила регламентируют действия руководства и сотрудников, участвующих в процессе внутреннего аудита по информационной безопасности.
3. Пересмотр и внесение изменений в данные Правила осуществляются согласно делопроизводству.
4. Настоящие Правила вступают в действие с момента утверждения.

## 2. Нормативные ссылки

5. При разработке данных Правил использованы следующие нормативные документы и формы качества:

- СТ РК ИСО 9001-2016 Система менеджмента качества. Требования.
- СТ РК ИСО/МЭК 27001:2015 Методы и средства обеспечения безопасности системы управления информационной безопасностью.

## 3. Термины и сокращения

**Организация** - ОЮЛ Ассоциация ВИЭ «Qazaq Green»;

**ИС** – информационная система «Торговая платформа для товарных и сырьевых бирж Казахстана» 2.0;

**Критерии аудита –** совокупность политик, процедур и требований;

**Свидетельство аудита –** записи, изложения фактов или другая информация, которая связана с критериями аудита и может быть проверена;

**Аудит –** систематический независимый и документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнения согласованных критериев аудита;

**Аудитор** – сотрудник Организации, назначенный приказом Первого руководителя, и уполномоченный проводить внутренний аудит;

**Внутренний аудит** – внутренний аудит системы управления информационной безопасностью;

**СМК** – система менеджмента качества;

**СУИБ** – система управления информационной безопасностью;

**Специалист по информационной безопасности** – сотрудник Организации, ответственный за информационную безопасность;

**Несоответствие** – невыполнение требования утвержденного регламентирующего документа;

**Коррекция** – устранение выявленного несоответствия;

**Корректирующие действия** – действие, предпринятое для устранения причины обнаруженного несоответствия или другой потенциально нежелательной ситуации;

**Предупреждающие действия** – действие, предпринятое для устранения причины потенциального несоответствия или другой потенциально нежелательной ситуации;

## 4. Общие положения

6. Владельцем процесса является специалист по информационной безопасности.

7. Внутренний аудит проводится с целью:

1) проверки соответствия СУИБ требованиям стандарта СТ РК ИСО/МЭК 27001:2015;

2) подтверждения того, что СУИБ в Организации внедряется или внедрена и поддерживается в рабочем состоянии;

3) демонстрации того, насколько близко к правилам, установленным в процедурах СУИБ, выполняется работа в Организации и есть ли различия между реальной работой и тем, что установлено в документации СУИБ.

8. Аудит может быть двух видов:

1) плановый аудит;

2) внеплановый аудит.

9. Результаты аудита предоставляются руководству для разработки корректирующих и/или предупреждающих действий.

10. К записям по аудиту относятся:

1) годовой план внутреннего аудита;

2) программа проведения внутреннего аудита;

3) чек – лист;

4) отчет по результатам внутреннего аудита.

11. Формы записей по аудиту, приведенные в приложениях к настоящему руководству носят рекомендательный характер и могут быть изменены в зависимости от специфики бизнес-процесса Организации.

## 5. Порядок проведения внутреннего аудита

### 5.1. Планирование внутреннего аудита

12. Внутренний аудит осуществляется аудиторами в соответствии с утвержденным годовым планом внутреннего аудита согласно **Приложению 1** к настоящим Правилам.

13. Годовой план внутреннего аудита разрабатывается специалист по информационной безопасности, согласовывается с системным администратором и утверждается Первым руководителем Организации, не позднее 15 декабря текущего года.

14. Копии утвержденного годового плана внутреннего аудита рассылаются каждому проверяемому сотруднику не позднее 20 декабря текущего года.

15. Проведение внеплановых внутренних аудитов может проводиться по упрощенному порядку, без оформления письменного уведомления и Плана аудита, но с обязательным оформлением результатов аудита в соответствии с настоящими Правилами.

### 5.2. Подготовка группы внутренних аудиторов

16. Аудиторы выбираются исходя из принципа: Аудитор не должен проверять своего непосредственного начальника.

17. Специалист по информационной безопасности несет ответственность за все этапы аудита.

18. Руководство Организации должно способствовать повышению квалификации аудиторов.

19. При определении размера и состава группы для проведения внутреннего аудита ИБ учитывается компетентность проверяющей группы, в основе которой лежит уровень квалификации ее участников.

20. Производится распределение ролей и обязанностей по проведению внутреннего аудита Организации между членами аудиторской группы. Формируются основные группы, непосредственно занимающиеся аудитом (проверкой) знаний сотрудников и выполнений ими требований нормативных документов, положений Организации в отношении ИБ и непосредственно аудитом нормативных документов, определяющих информационную безопасность Организации.

21. Группа аудиторов обеспечивается рабочими местами, всей необходимой нормативно-технической документацией (политика, акты, протоколы, договора и пр.).

22. При проведении внутреннего аудита ИБ применяется соответствующее инструментальное обеспечение. Инструментальное обеспечение, используемое при аудите ИБ, может включать средства автоматизации анализа выполнения требований ИБ.

23. Инструментальные средства автоматизации анализа выполнения требований ИБ (критериев аудита ИБ) должны позволять:

- автоматизировать процесс оценки степени выполнения требований ИБ с учетом их важности;
- оценивать эффективность различных вариантов защитных мер;
- автоматизировать процессы анализа идентифицированных и зафиксированных внештатных действий пользователей и инцидентов ИБ;
- генерировать документальные отчеты с результатами выполнения различных процедур.

### 5.3 Инструментальный аудит ИБ

24. Инструментальный аудит – выявление уязвимостей программно-аппаратных средств методами автоматизированной проверки.

25. Основным этапом в проведении инструментального аудита является сбор всех необходимых данных обо всех информационных активах:

– перечень серверов, рабочих станций и коммуникационного оборудования;
– информация о периферийном оборудовании;
– информация об операционных системах, установленных на рабочих станциях и серверах;
– данные о СУБД;
– перечень прикладного ПО;
– информация о производителе средства защиты;
– конфигурационные настройки средства защиты;
– схема установки средства защиты;
– информация о типах каналов связи;
– информация об используемых сетевых протоколах, IP-адресов;
– схема информационных потоков

26. Инструментальный анализ защищённости проводится для выявления технологических уязвимостей в программно-аппаратном обеспечении ИС.

27. В процессе инструментального аудита используются специализированные программные средства. Сетевое сканирование реализуется в два основных этапа. На первом этапе осуществлялся сбор

исходной информации о хосте, включающей в себя перечень открытых портов, информацию о типе сетевых служб, запущенных на хосте и т.д.

28. На втором этапе проводится поиск уязвимостей именно в той сетевой службе, которая является основной в работе данного сервера (Например – web-сервер).

29. В рамках инструментального аудита также проводится анализ конфигурационных настроек общесистемного и прикладного программного обеспечения. Данный аудит направлен на выявление эксплуатационных уязвимостей, к которым относятся ошибки в настройке программного или аппаратного обеспечения.

30. На заключительном этапе формируется Отчет о результатах инструментального аудита защищенности и общие рекомендации по устранению выявленных недостатков в процессах обеспечения ИБ.

### 5.4. Проведение аудита

31. Специалист по информационной безопасности за 7 рабочих дней должен известить проверяемого о проведении внутреннего аудита в любой доступной форме и ознакомить с программой аудита, оформленной согласно **Приложению 2**.

32. В качестве цели аудита может быть указано следующее:

- проверка исполнения требований утвержденного регламентирующего документа;
- проверка соответствия деятельности требованиям утвержденных регламентирующих документов.

33. Оригинал программы аудита хранится у специалиста по информационной безопасности.

34. Проверяемые в свою очередь обязаны довести до сведения заинтересованных лиц информацию о предстоящем аудите.

35. В случае невозможности проведения аудита в установленное планом аудита время, необходимо поставить в известность внутреннего аудитора в электронной форме, указав причину переноса, который принимает решение о переносе срока данного аудита. Срок переноса не должен превышать одного месяца.

36. В процессе проведения внутреннего аудита аудиторы производят сбор объективных свидетельств соответствия процессов утвержденным регламентирующим документам посредством опроса работников Организации, изучения документов и проведения наблюдений.

37. Данные, полученные в ходе внутреннего аудита, аудитор должен фиксировать в чек-листах согласно **Приложению 3** к настоящим Правилам.

Вопросы в графе 2 должны обеспечивать получение достоверной и полной информации, подтверждающей наличие или отсутствие доказательств соответствия требованиям, предусмотренным программой аудита.

38. По итогам внутреннего аудита аудитор составляет отчет по результатам внутреннего аудита согласно **Приложению 4** к настоящим Правилам и направляет его копию проверяемому.

39. Каждый отчет о несоответствии аудитор регистрирует в Журнале регистрации отчетов о несоответствии и передает проверяемому.

40. Проверяемый в течение 3 календарных дней после получения отчета о несоответствии разрабатывает корректирующие/предупреждающие действия и направляет его специалисту по информационной безопасности. Период устранения несоответствий определяется проверяемым, но не должен превышать 1 месяца.

41. По истечению сроков устранения несоответствий специалист по информационной безопасности проводит внеплановый аудит и делает пометку в отчете о несоответствии и в Журнале регистрации отчетов о несоответствии.

42. Записи по аудиту должны поддерживаться в рабочем состоянии и хранится у специалиста по информационной безопасности.

43. Контроль выполнения годового плана внутреннего аудита осуществляет системным администратором и специалистом по информационной безопасности, согласно своей сферы деятельности.

44. Контроль выполнения корректирующих/предупреждающих действий по результатам внутреннего аудита проводит специалист по информационной безопасности.

## 6. Ответственность

45. Ответственным за организацию проведения внутренних аудитов является специалист по информационной безопасности.

46. Специалист по информационной безопасности несет ответственность за хранение записей по внутреннему аудиту.

47. Специалист по информационной безопасности несет ответственность за разработку и актуализацию настоящих Правил.

48. Аудиторы несут ответственность за неразглашение конфиденциальной информации, полученной в ходе внутренних аудитов.

49. Системный администратор несет ответственность за проверку выполнения требований настоящих Правил.

50. Проверяемые несут ответственность за разработку и своевременное выполнение корректирующих/предупреждающих действий по результатам внутренних аудитов.

51. Проверяемые несут ответственность за неисполнение/ненадлежащее исполнение требований СУИБ, изложенных в настоящих Правилах.

## 7. Критерии качества СУИБ

52. Следующие критерии качества используются при формировании отчета для анализа со стороны руководства:

| № п | Наименование критерия | Ед. изм. | Формула |
|---|---|---|---|
| 1. | Выполнение годового плана аудита | % | (проведенные плановые аудиты/запланированные аудиты)*100 |
| 2. | Количество выявленных несоответствий | шт | |

**Приложение 1**
к Правилам проведения внутреннего аудита
информационной безопасности
«__» _____ 202_ г. № __

**УТВЕРЖДАЮ**
**Директор _____**
**«____» _____ 202_ г.**

**Годовой план внутреннего аудита на 202_ год.**

| № п/п | Цель аудита | Проверяемое | Месяцы года | | | | | | | | | | | | Фамилия И.О. внутреннего аудитора | Примечания |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | Январь | Февраль | Март | Апрель | Май | Июнь | Июль | Август | Сентябрь | октябрь | Ноябрь | Декабрь | | |
| | | | Числа месяца | | | | | | | | | | | | | |
| 1 | 2 | 3 | 4 | | | | | | | | | | | | 5 | 6 |
| | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | |

**ПОДГОТОВИЛ:** _____ _____ _____
должность *(подпись)* *(Ф.И.О.)*

**СОГЛАСОВАНО:** Системный администратор _____ _____
*(подпись)* *(Ф.И.О.)*

**Приложение 2**
к Правилам проведения внутреннего аудита
информационной безопасности
«__» _____ 202_ г. № __

**Программа**
**проведения внутреннего аудита**

_____

*Должность проверяемого (или наименование структурного подразделения)*

**1. Время и дата начала аудита _____ «____» _____ 20___ год**
**2. Время и дата завершения аудита_____ «____» _____ 20___ год**
**3. Цель аудита: _____**
**_____**

**Критерии аудита: _____**
**_____**
**_____**

**4. Аудит проводится в соответствии с требованиями**

| № | Пункт регламентирующего документа | Вопросы |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**Внутренний аудитор** _____ _____ _____
*подпись* *ФИО* *дата*

**Ответственный за проведение аудита (проверяемый)** _____ _____ _____
*подпись* *ФИО* *дата*

**Приложение 3**
к Правилам проведения внутреннего аудита
информационной безопасности
«__» _____ 202_ г. № __

**Чек – лист**

_____

*Должность проверяемого (или наименование. структурного подразделения)*
**«____» _____202_ г.**

| **Пункты стандартов СТ РК ИСО/МЭК 27001:2015** | **Вопрос** | **Наблюдение аудитора** |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

**Внутренний аудитор** _____ _____ _____
*подпись* *ФИО* *дата*

**Приложение 4**
к Правилам проведения внутреннего аудита
информационной безопасности
«__» _____ 202_ г. № __

**Отчет**
**по результатам внутреннего аудита № ___**

**Раздел 1.**
1. Проверяемый (или структурное подразделение):
_____
_____
2. Аудитор:
_____
3. Период аудита с _____ по _____
*дата* *дата*

**Раздел 2.**
Цель аудита:
_____

**Раздел 3.**
Критерии аудита:
_____
_____

**Раздел 4.**
Результаты аудита:
1. Несоответствие (значительное/незначительное):
_____
_____

2. Рекомендации по результатам внутреннего аудита:
_____
_____

**Проверяемый** _____ _____ _____
*подпись* *ФИО* *дата*

**Внутренний аудитор** _____ _____ _____
*подпись* *ФИО* *дата*

## ЛИСТ ОЗНАКОМЛЕНИЯ

| № | Фамилия, имя, отчество | Должность | Личная подпись | Дата |
|---|---|---|---|---|
| **1** | **2** | **3** | **4** | **5** |
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |
| 6 | | | | |
| 7 | | | | |
| 8 | | | | |
| 9 | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |