«УТВЕРЖДЕНО»
Решением Правления
НАО «Университет Нархоз»
Протокол № 8 от
«15». 06 .2023 г.

Правила проведения внутреннего аудита информационной безопасности IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»

Алматы, 2023

Оглавление

Паспорт документа

Наименование документа:	Правила проведения внутреннего аудита информационной безопасности IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Краткое описание:	Правила проведения внутреннего аудита информационной безопасности IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Тема:	Информационная безопасность
Статус:	Новый
Дата утверждения:	«___» _____2023г.
Дата завершения действия:	
Дата аудита:	Ежемесячно
Ответственный за аудит:	Эксперт по информационной безопасности

Лист согласования

Должность	Ф.И.О.	Подпись
Директор Административного департамента	Бисенгали Л	
Советник по цифровизации	Тебаев Д.Б.	
и.о. Директора Департамента информационных технологий	Жумажанов Б.Ж.	

1 Назначение документа

1.1 Настоящие Правила проведения внутреннего аудита информационной безопасности IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз» (далее – «Правила») разработаны в соответствии с СТ РК ИСО/МЭК 27001, а также иными нормативно-правовыми актами и стандартами Республики Казахстан, и регламентируют порядок проведения внутреннего аудита информационной безопасности IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз» (далее – «Общество»).

1.2 Целями внутреннего аудита информационной безопасности (далее – «ИБ») Общества являются:

- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз» (далее – «ITA»);
- оценка текущего уровня защищенности IT;
- локализация узких мест в системе защиты ITA;
- оценка соответствия ITA существующим стандартам в области ИБ ТОО «Verny Capital» VC 04.04.2022;
- выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности ITA.

1.3 Периодичность проведения внутреннего аудита ИБ Общества и его структурных подразделений определяется руководством Общества на основе потребностей в такой деятельности.

1.4 Аудит на предмет исполнения и соблюдения требований информационной безопасности можно подразделить на следующие виды проверок:

- аудит ресурсов ITA, корпоративной вычислительной сети с целью подготовки технического задания на проектирование и разработку системы защиты информации;
- аудит ITA, корпоративной вычислительной сети, после внедрения системы безопасности для оценки уровня её эффективности;
- профилактический регулярный аудит, направленный на приведение действующей системы безопасности в соответствие требованиям нормативных правовых актов Республики Казахстан;
- аудит, предназначенный для систематизации и упорядочивания существующих мер защиты информации;
- аудит (служебное расследование) в целях расследования произошедшего инцидента, связанного с нарушением требований информационной безопасности;
- совместный аудит, проводимый с экспертом по ИБ ТОО «Verny Capital».

1.5 Аудит на предмет исполнения и соблюдения требований информационной безопасности подразделяется на плановый и внеплановый.

1.6 Плановый аудит на предмет исполнения и соблюдения требований информационной безопасности проводится согласно утвержденному плану-графику планового аудита, который составляется ежегодно экспертом по ИБ и утверждается приказом руководителя Общества. Форма Плана-графика приведена в Приложении № 1 к настоящим Правилам. План-график внутренних аудитов включает в себя все аудиты, планируемые Специалистом ИБ к проведению в течение года, и содержит требования к видам деятельности в ходе аудита, срокам выполнения и необходимым ресурсам.

1.7 Процедура проведения планового аудита включает в себя следующие мероприятия:

- аудит проводится в соответствии с графиком аудита;
- план аудита составляется экспертом по ИБ. План аудита должен содержать перечень мероприятий, которые необходимо провести при проведении аудита (в качестве

запланированных мероприятий могут быть аудит исполнения нормативно правовых актов по информационной безопасности, утвержденных в Обществе, проведение сканирования, диагностирования технического оборудования и т.д.);

• методы сбора информации могут включать интервьюирование работников, заполнение опросных листов, анализ предоставленной организационно-распорядительной и технической документации, использование специализированных инструментальных средств;

• после окончания аудита проводится анализ собранной информации, с целью оценки текущего уровня защищённости объекта проверки. По результатам проведённого анализа, руководству подразделения ответственного за объект аудита выдается рекомендация по устранению нарушений;

1.8 Внеплановый аудит на предмет исполнения и соблюдения требований информационной безопасности проводятся на основании составленных актов о выявленных нарушениях с резолюцией руководства Общества.

2 Ссылки

2.1 Настоящие Правила разработаны в соответствии со следующими нормативно-правовыми актами и документами:

• Закон Республики Казахстан «Об информатизации» от 24.11.2015г.;

• Постановление Правительства Республики Казахстан от 20.12.2016г. №832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности;

• СТ РК ИСО/МЭК 27002 «Методы обеспечения защиты. Свод правил по управлению защитой информации»;

• СТ РК ИСО/МЭК 27001 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»;

• СТ РК ГОСТ Р 50739 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования».

• Стандарт по информационной безопасности ТОО «Verny Capital».

3 Требования к аудиторской группе

3.1 Для проведения внутреннего аудита ИБ должна быть подобрана аудиторская группа. Руководством Общества должен быть назначен руководитель аудиторской группы, ответственный за проведение аудиторской проверки. При наличии только одного аудитора, последний должен выполнять все предусмотренные обязанности руководителя аудиторской группы.

3.2 При определении размера и состава аудиторской группы должны учитываться:

• цели, область аудита ИБ, критерии аудита и его ориентировочная продолжительность;

• общая компетентность и уровень квалификации аудиторской группы;

• необходимость исполнения принципов проведения аудита ИБ;

• законодательные, регламентирующие, контрактные требования;

• способность членов аудиторской группы к совместной работе и к эффективному взаимодействию с проверяемой организацией;

• понимание социальных и культурных особенностей Общества и ее структурных подразделений (это может быть достигнуто либо собственным опытом аудитора, либо с помощью эксперта).

3.3 Если в определенной области (по определенному вопросу) знаний

аудиторской группы недостаточно, то недостающие знания и умения могут быть восполнены включением в группу экспертов. Эксперты должны работать под руководством аудитора.

3.4 Для взаимодействия с аудиторской группой руководством проверяемой организации должны быть назначены лица, на которых возлагается ответственность за своевременность, достоверность и полноту предоставления запрошенной аудиторами информации в объеме, не выходящем за пределы их полномочий.

3.5 При проведении внутреннего аудита (планового и внепланового) члены аудиторской группы имеют право:

- беспрепятственного допуска в служебные помещения проверяемых объектов;
- беспрепятственного доступа к необходимой информации, которой располагает Общество, включая компьютерные системы, для осуществления внутреннего аудита. Данное право в отношении информации, содержащей сведения, составляющие государственную тайну, может быть реализовано в порядке, установленном для работы с документами, составляющими государственную тайну;
- получения отчетов о результатах аудиторской проверки внешних аудиторов;
- расширения круга вопросов (участков) проверки, если выявляется необходимость в таком расширении при выполнении программы проверки;
- копирования отдельных документов, в том числе получения копий файлов;
- получения любых записей, хранящихся в локальных вычислительных сетях и автономных компьютерных системах, а также получения расшифровки этих записей. Данное право в отношении информации, содержащей сведения, составляющие государственную тайну, может быть реализовано в порядке, установленном для работы с документами, составляющими государственную тайну;
- получения от работников проверяемых участков устных и письменных объяснений по вопросам, возникающим в ходе проведения проверки;
- в случаях предоставления недостоверных документов, отказа в предоставлении информации или письменных обоснований, создания иных препятствий проведению внутреннего аудита члены аудиторской группы докладывают руководителю аудиторской группы, который обращается к руководству Общества с требованием о принятии мер ответственности к лицам, виновным в создании препятствий проведению внутреннего аудита;
- вносить для рассмотрения руководству Общества предложения по результатам внутреннего аудита, проведённого в структурных подразделениях.

4 **Порядок проведения внутреннего аудита**

4.1 На основании утвержденного Плана-графика внутренних аудитов формируются программы проведения конкретных проверок – Программы аудита. Форма Программы аудита приведена в Приложении №2 к настоящим Правилам. Ответственность за разработку Программы аудитов возлагается на Руководителя аудиторской группы.

4.2 При разработке Программы аудита определяются:

- критерии аудита;
- состав аудиторской группы;
- область аудита (подразделения и участки, которые предстоит посетить аудиторам);
- сроки проверок.

4.3 Руководитель аудиторской группы знакомит с разработанной Программой аудита всех членов аудиторской группы. После этого не менее чем за 7 (семь) рабочих дней до проведения аудита Программа аудита передается руководителям проверяемых

подразделений для согласования условий и времени проведения аудита. В процессе согласования условия и время проведения аудита могут быть изменены по обоснованной просьбе руководителя проверяемого подразделения. Согласованная Программа аудита передается на утверждение руководству Общества.

4.4 Далее проводится подготовка к проведению аудита, включающая в себя:

- ознакомление аудиторов с критериями аудита;
- изучение и анализ документации, действующей в области аудита;
- подготовку рабочих документов – опросных листов.

4.5 Ознакомление аудиторов с критериями аудита предусматривает изучение политики, процедур, требований, определенных в плане проверки.

4.6 Осуществление аудита в подразделении предусматривает:

- проведение вводного совещания;
- обследование объекта аудита;
- составление заключения о результатах аудита;
- проведение заключительного совещания.

4.7 Вводное совещание проводит руководитель проверяемого подразделения совместно с руководителем группы по аудиту для того, чтобы:

- разъяснить цели и методы аудита;
- установить официальные средства общения между членами аудиторской группы и работниками проверяемого подразделения;
- уточнить неясные детали аудита;
- сформировать позитивные отношения к аудиту.

4.8 Основными задачами обследования объекта аудита является получение объективных данных о выполнении требований ИБ. Полученные данные должны оцениваться для определения степени выполнения требований ИБ.

4.9 По окончании проверки в подразделении руководитель группы по аудиту организует и проводит совместно с руководителем подразделения заключительное совещание с целью доведения до сведения руководства проверяемого подразделения результатов работы.

4.10 После выполнения программы аудита руководитель группы по аудиту, совместно с группой аудиторов оформляют отчет по аудиту. Форма отчета по аудиту приведена в Приложении №3 к настоящим Правилам.

4.11 Ответственность за проведение внутренних аудитов, согласно утвержденной программы аудитов, несет руководитель аудиторской группы.

4.12 Все спорные и конфликтные ситуации, возникающие в процессе проведения проверки между руководителем аудиторской группы и проверяемым объектом, разрешаются руководителем ответственного подразделения, в особых случаях – руководителем Общества.

5 Инструментальное обеспечение внутреннего аудита информационной безопасности

5.1 При проведении внутреннего аудита ИБ должно применяться соответствующее инструментальное обеспечение. Инструментальное обеспечение, используемое при аудите ИБ, может включать средства автоматизации анализа выполнения требований ИБ и средства автоматизации оценки рисков.

5.2 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;

5.3 Инструментальные средства автоматизации оценки рисков должны позволять:

• анализировать выполнение политики ИБ в организации;

• оценивать риски с использованием принятых подходов и методик, утвержденных уполномоченным органом в области технической защиты информации;

• идентифицировать и оценивать варианты корректировки риска;

• вырабатывать рекомендации по методам и средствам снижения риска при сборе, обработке, хранении конфиденциальной информации;

• вырабатывать и предоставлять обоснования для выбора защитных мер;

• генерировать отчеты по результатам оценки.

6 Ответственность

6.1 Все участники внутреннего аудита информационной безопасности IT инфраструктуры обязаны соблюдать конфиденциальность и не разглашать полученную информацию третьим лицам без предварительного разрешения.

6.2 Руководитель аудиторской группы информационной безопасности должен обеспечить назначение ответственных лиц для выполнения каждого этапа аудита, а также контролировать их деятельность и своевременное выполнение задач.

6.3 Ответственные лица, проводящие аудит, должны иметь соответствующую квалификацию и опыт в области информационной безопасности, а также следовать процедурам и методологии аудита, установленным в организации.

6.4 Результаты аудита должны быть представлены руководству организации с подробными отчетами и рекомендациями по улучшению информационной безопасности IT инфраструктуры.

7 Заключительные положения

a. Руководитель аудиторской группы информационной безопасности должен подготовить заключительный отчет, который должен содержать обзор выполненных работ, выявленные уязвимости и рекомендации по улучшению информационной безопасности IT инфраструктуры.

b. Руководство организации должно рассмотреть заключительный отчет и принять меры по исправлению выявленных проблем и реализации рекомендаций.

c. После завершения аудита информационной безопасности IT инфраструктуры, руководитель аудиторской группы должен провести финальную встречу с руководством организации для обсуждения результатов аудита и ответов на вопросы.

Приложение 1 к
Правилам проведения внутреннего аудита информационной безопасности IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»

«УТВЕРЖДАЮ»

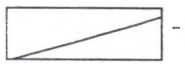
_____ _____

План-график внутренних аудитов на _____ год

Наименование подразделений	**Объект аудита**	**Дата предыдущего аудита**	**Отметка о плановой и фактически проведенной проверке (неделя)**											
			январь	**февраль**	**март**	**апрель**	**май**	**июнь**	**июль**	**август**	**сентябрь**	**октябрь**	**ноябрь**	**декабрь**

Примечание: В случае возникновения в подразделениях сбойных ситуаций, неучтенных опасностей и рисков проводится дополнительная внеплановая проверка.

Представитель руководства _____

Условные обозначения:  - плановая проверка (неделя месяца)  - фактически проведенная проверка

Приложение 2 к Правилам проведения внутреннего аудита информационной безопасности IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»

ПРОГРАММА АУДИТА № _____
№ _ по плану-графику аудитов

1. Наименование структурного подразделения: _____
2. Цель аудита _____
3. Сроки проведения аудита _____
4. Задачи аудита _____
5. Состав группы: _____
6. Перечень нормативных документов: _____
_____
_____
7. Дата представления отчета _____
8. Отчет печатать в _____экз.

Руководитель аудиторской группы _____ _____ _____
(подпись) (дата) (Ф.И.О.)

Аудиторы _____ _____ _____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО
Руководитель проверяемого подразделения _____ _____ _____
(подпись) (дата) (Ф.И.О.)

Приложение 3 к Правилам проведения внутреннего аудита информационной безопасности IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»

ОТЧЕТ О ВНУТРЕННЕМ АУДИТЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
№ ___ по плану аудитов

1. Наименование структурного подразделения_____
2. Руководитель подразделения_____
3. Руководитель аудиторской группы _____
4. Аудиторы _____
5. Дата аудита _____
6. Раздел/ документ (ы), на соответствие которому (ым) проводится аудит _____
_____
7. РЕЗУЛЬТАТЫ АУДИТА:
Количество выявленных «высоких» несоответствий _____
_____
Количество выявленных «средних» несоответствий _____
_____
Количество выявленных «низких» несоответствий _____
_____
Количество предложений _____

8. ЗАКЛЮЧЕНИЕ ПО РЕЗУЛЬТАТАМ АУДИТА:
Деятельность_____ удовлетворяет (не удовлетворяет) установленным требованиям _____
Корректирующие мероприятия (план) _____

Необходимость повторного аудита: ДА/НЕТ по документу _____

Составил
Руководитель аудиторской группы _____ _____
(подпись, дата) (И.О. Фамилия)
Согласовано:
Представитель руководства _____ _____
(подпись, дата) (И.О. Фамилия)

ЛИСТ ОЗНАКОМЛЕНИЯ

№	Фамилия, имя, отчество	Должность	Подпись	Дата
1	2	3	4	5