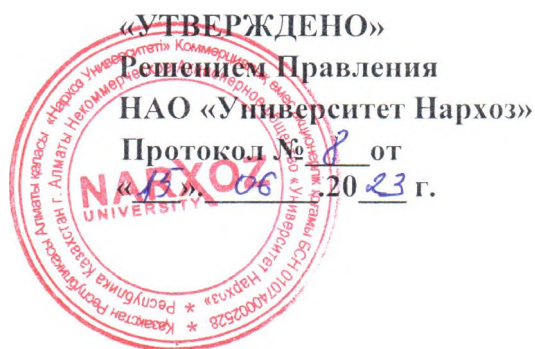


**«УТВЕРЖДЕНО»**  
**Решением Правления**  
**НАО «Университет Нархоз»**  
**Протокол № 8 от**  
**«13» 06 2023 г.**



**Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях Некоммерческого акционерного общества «Университет Нархоз»**

## Оглавление

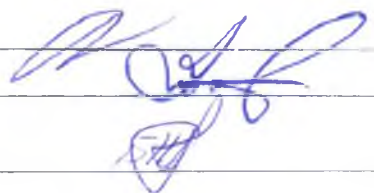
Паспорт документа .....	3
Лист согласования.....	4
1. Область применения .....	5
2. Понятия и сокращения .....	5
3. Ссылки.....	5
4. Перечень возможных внештатных ситуаций, идентификация и порядок действия по устранению .....	5
5. Контроль возникновения внештатных (кризисных) ситуаций и корректирующих действий по ним .....	8
6. Проведение расследований в случае возникновения инцидентов и других внештатных ситуаций .....	9
7. Ответственность .....	9
8. Заключительные положения .....	9

## Паспорт документа

---

<b>Наименование документа:</b>	Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях Некоммерческого акционерного общества «Университет Нархоз»
<b>Краткое описание:</b>	Инструкция о порядке действий пользователей по реагированию на инциденты информационной безопасности и во внештатных (кризисных) ситуациях Некоммерческого акционерного общества «Университет Нархоз»
<b>Тема:</b>	Информационная безопасность
<b>Статус:</b>	Новый
<b>Дата утверждения:</b>	«___» _____ 2023г.
<b>Дата завершения действия:</b>	Ежегодно
<b>Дата аудита:</b>	Эксперт по информационной безопасности
<b>Ответственный за аудит:</b>	

Лист согласования

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

## 1 Область применения

1.1 Настоящая Инструкция (далее – «Инструкция») предназначена для обслуживающего персонала, при возникновении внештатных (кризисных) ситуаций ИТ инфраструктуры НАО «Нархоз» (далее – «ИТА») Некоммерческого акционерного общества (далее – «Общество»).

## 2 Понятия и сокращения

**ИТ инфраструктура (ИТА)** – совокупность информационных технологий, информационных сетей и средств их программно-технического обеспечения, предназначенных для реализации информационных процессов;

**ИБ** – Информационная безопасность;

**ПК** – Персональный компьютер;

**ПО** – Программное обеспечение;

**ППО** – Прикладное программное обеспечение;

**ОС** – Операционная система;

**Администратор** – Лицо/лица, осуществляющее администрирование информационной системы;

**Пользователь** – Пользователь информационной системы;

**СВТ** – Средства вычислительной техники;

**СУБД** – Система управления базами данных;

**СТО** – Сервисное техническое обслуживание.

## 3 Ссылки

3.1. Настоящая Инструкция разработана на основании следующих документов:

- 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».

## 4 Перечень возможных внештатных ситуаций, идентификация и порядок действия по устранению

4.1. Внештатная ситуация может возникнуть в результате злого умысла или случайно (в результате непреднамеренных действий, аварий, стихийных бедствий и т.п.). По степени серьезности и размерам наносимого ущерба внештатные ситуации разделяются на следующие категории:

Угрожающая – приводящая к полному ИТА из строя и неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации;

Серьезная – приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного

доступа.

4.2. Ситуации, возникающие в результате нежелательных воздействий, не наносящих ощутимого ущерба, но, тем не менее, требующие внимания и адекватной реакции (например, зафиксированные неудачные попытки прощипновения или несанкционированного доступа к ресурсам системы) к критическим не относятся.

4.3. К внештатным ситуациям, например, могут быть отнесены:

- отключение электричества. Администраторы ИТА проводят анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости производится восстановление ПО и данных из последней резервной копии с составлением акта;

- выход из строя сервера. Администратор ИТА, проводит меры по немедленному вводу в действие резервного сервера для обеспечения непрерывной работы управления. При обнаружении потери данных Администраторы ИТА проводят мероприятия по поиску и устранению причин потери данных (антивирусная проверка, целостность и работоспособность ПО, целостность и работоспособность оборудования и др.). Производится восстановление ППО и данных из резервных копий с составлением акта;

- сбой в локальной вычислительной сети. Администратор ИТА проводят анализ на наличие потерь и (или) разрушения данных и ПО. В случае необходимости, производится восстановление ПО и данных из последней резервной копии с составлением акта;

- возгорание в серверном помещении.

4.4. Ситуация 1: Недоступность ИТА для пользователей

Описание	Ситуация, когда пользователи по ряду причин не могут работать с ИТА к таковым причинам могут относиться выход из строя сервера или сетевого оборудования, коммуникаций, сбой программного обеспечения.
Действия по идентификации: (Администратор АИС)	1. Необходимо выяснить, действительно ли недоступность ИТА для пользователя связана со сбоем в функционировании АИС. 2. Принять меры по определению причины недоступности ИТА. В случае, если недоступность ИТА обусловлена сбоем в функционировании ИТА, необходимо переходить к действиям по устранению
Действия по устранению:	1. Поставить в известность непосредственное руководство о возникшей ситуации с недоступностью ИТА. 2. Самостоятельно или совместно, при участии обслуживающего персонала ИТА устранить причину недоступности ИТА. 3. Сделать отметку в электронном журнале регистрации внештатных ситуаций.

4.5. Ситуация 2: Воздействие природно-климатических условий

Описание	Ситуации возникновения стихийных природно-климатических воздействий (землетрясение, наводнения, ураганы и т.д.).
Действия по идентификации:	В случае, если в непосредственной близости от здания, где размещены сервера ИТА наблюдаются стихийные природно-климатические воздействия (землетрясение, наводнения, ураганы и т.д.) необходимо осуществить нижеуказанные действия.
Действия по	1. Поставить в известность руководство;

устранению:	<ol style="list-style-type: none"> <li>2. По возможности корректно отключить сервера ИТА;</li> <li>3. По возможности вынести резервные копии ИТА;</li> <li>4. Сообщить в органы по чрезвычайным ситуациям (тел.: 112);</li> <li>5. Сделать отметку в электронном журнале регистрации внештатных ситуаций;</li> <li>6. Организованно покинуть здание в соответствии с планом эвакуации.</li> </ol>
-------------	---

#### 4.6. Ситуация 3: Пожар или возгорание

Описание	Ситуации при возникновении пожара или возгорания
Действия по идентификации:	В случае, если в непосредственной близости серверов ИС наблюдается пожар или возгорание необходимо переходить к действиям по устранению
Действия по устранению:	<ol style="list-style-type: none"> <li>1. Вызвать пожарную службу;</li> <li>2. Поставить в известность руководство;</li> <li>3. По возможности корректно отключить сервера ИС;</li> <li>4. Проконтролировать запуск системы автоматического пожаротушения;</li> <li>5. Если возник сбой в запуске системы автоматического пожаротушения, то осуществить ее запуск в ручном режиме;</li> <li>6. Сделать отметку в электронном журнале регистрации нештатных ситуаций. При выполнении дальнейших действий необходимо руководствоваться утвержденными в организации инструкциями по действиям при пожаре.</li> </ol>

#### 4.7. Ситуация 4: Нарушение политики информационной безопасности заявителя

Описание	Ситуация при нарушении требований политики информационной безопасности ИТА
Действия по идентификации:	В случае, если наблюдается факт нарушения требований политики ИТА, необходимо переходить к действиям по устранению.
Действия по устранению:	<ol style="list-style-type: none"> <li>1. Поставить в известность ответственного по ИБ и руководство о возникшей ситуации ИТА;</li> <li>2. Выявить и устранить причину нарушения требований политики информационной безопасности ИТА».</li> </ol>

#### 4.8. Действия при возникновении ситуаций, не подпадающих под перечисленный список

В случае возникновения важных, критических или внештатных ситуаций с ИТА, не подпадающих под вышеперечисленный список администратору ИТА необходимо:

- поставить в известность о возникшей внештатной ситуации ИТА директора ДИТ и ответственного по ИБ;
- при необходимости принять участие в устранении последствий внештатной ситуации;
- администратор ИТА делает отметку в электронном журнале регистрации внештатных ситуаций.

## 5 Контроль возникновения внештатных (кризисных) ситуаций и корректирующих действий по ним

5.1. Для выполнения профилактических действий, с целью предотвращения возникновения внештатных или кризисных ситуаций должны проводиться следующие мероприятия:

1. Администраторы ИТА должны ежедневно проводить мониторинг автоматизированных информационных систем, включающий в себя опрос состояния СУБД, ОС и ППО, с помощью специализированного программного обеспечения, в случае изменения состояния доступности автоматизированных информационных систем произойдет оповещение администратора в режиме «онлайн»;

2. Администратор ИТА должен ежедневно проводить мониторинг событий, связанных с нарушением ИБ, и анализ результатов мониторинга, в том числе:

- журналов событий операционных систем;
- журналов событий систем управления базами данных;
- журналов действий пользователей, влияющих на ИБ;
- журналов событий антивирусной защиты;
- журналов событий прикладного ПО;
- журналов событий телекоммуникационного оборудования.

3. Администраторы ИТА должны проводить резервное копирование информации в соответствии с регламентом резервного копирования и восстановления информации;

4. Администраторы ИТА должны осуществлять обновление программного обеспечения в соответствии с установленными правилами;

5. В случаях получения информации о возможных предстоящих внештатных ситуациях, должно быть обеспечено оперативное оповещение всех причастных лиц и структур.

6. Администраторы ИТА обязаны как можно быстрее сообщать о любых событиях в сфере информационной безопасности руководителю ДИТ и ответственному за ИБ и произвести соответствующую запись возникновения внештатных ситуаций в документе «Журнал учета внештатных ситуаций», указанном в Приложении 1 к настоящей Инструкции;

7. Каждая внештатная ситуация должна анализироваться ответственным за ИБ, совместно с руководителем ДИТ и Администраторами ИТА.

Осуществление контроля, за выполнением профилактических действий для предотвращения возникновения внештатных или кризисных ситуаций возлагается на ответственного по ИБ, и состоит из следующих мероприятий:

1) На еженедельной основе проводить контроль за ведением следующих журналов:

- журнал учета внештатных ситуаций;
- журнал регистрации и устранения уязвимостей ПО;
- журнал учета резервных копий;
- журнал учета изменений конфигурации оборудования;
- журнал тестирования и учета изменений СПО и ППО ИТА

2) На ежемесячной основе проводить анализ отчетов Администраторов ИТА о проделанной работе.

Ответственный за ИБ является ответственным лицом за оповещение работников Общества в случае возникновения внештатных (кризисных) ситуаций и инцидентов информационной безопасности.

Для эффективной реализации мероприятий по реагированию в случае внештатных ситуаций должны проводиться регулярные тренировки по различным внештатным ситуациям. По результатам тренировки в случае необходимости проводится уточнение настоящей Инструкции.



## **6 Проведение расследований в случае возникновения инцидентов и других внештатных ситуаций**

6.1 Для расследования опасных ситуаций в случаях, предусмотренных настоящей инструкцией может создаваться комиссия. В состав комиссии должны входить:

- ответственный по ИБ (председатель);
- руководитель ДИТ;
- администраторы ИТА;
- другие лица по решению председателя комиссии.

Деятельность комиссии должна по возможности происходить в режиме конфиденциальности.

6.2 В общем случае комиссия проводит:

- анализ и идентификацию причин инцидента, определение виновных;
- определение ущерба, нанесенного нештатной ситуацией;
- планирование мер для предотвращения повторения, нейтрализации последствий (если это возможно);
- анализ и сохранение доказательств, следов инцидента, улик и свидетельств;
- определение меры взыскания с виновного;
- взаимодействие, при необходимости с правоохранительными органами.

6.3 При сохранении улик, если есть возможность, Администраторами ИТА производится резервное копирование системной, служебной и конфиденциальной информации технических средств, вовлеченных в инцидент, включая логи (контрольные записи).

6.4 По результатам деятельности комиссии составляется акт с описанием ситуации. К акту прилагаются поясняющие материалы (копии экрана, распечатки журнала событий, и др.).

6.5 По результатам расследования Администраторами ИТА организуются мероприятия по реализации предложенных комиссией мер для предотвращения либо уменьшения вероятности проявления, подобных инцидентов в дальнейшем.

6.6 При проведении расследований, кроме того, необходимо ответить на следующие вопросы:

- можно ли было предупредить нештатную ситуацию?
- вызвана ли она слабостью средств защиты и регистрации?
- это первая кризисная ситуация такого рода?
- достаточно ли имеющегося резерва?
- есть ли необходимость пересмотра системы защиты?
- есть ли необходимость пересмотра настоящей инструкции?

## **7 Ответственность**

7.1. Ответственными за постоянный контроль выполнения требований настоящей Инструкции являются:

- ответственный по ИБ в части общего контроля информационной безопасности;
- руководитель ДИТ в части задач, возложенных на него настоящей инструкцией;
- администраторы ИТА в части задач, возложенных на них настоящей инструкцией.

В случае нарушения требований настоящей Инструкции ответственные лица привлекаются к дисциплинарной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

## **8 Заключительные положения**

8.1. Настоящая Инструкции утверждаются решением Правления.

8.2. Изменения и дополнения в настоящую Инструкцию вносятся решением Правления.

**Приложение 1  
к настоящей Инструкции о порядке  
действий пользователей по  
реагированию на инциденты ИБ во  
внештатных (кризисных) ситуациях**

**Журнал учета внештатных ситуаций**

<b>№</b>	<b>Дата возникновения ситуации</b>	<b>Дата устранения ситуации</b>	<b>Описание ситуации</b>	<b>Принятые меры к устранению</b>	<b>Ответственный исполнитель</b>

