|  |
| --- |
| МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ КАЗАХСТАН |
| **С.Ж. АСФЕНДИЯРОВ АТЫНДАҒЫ****ҚАЗАҚ ҰЛТТЫҚ МЕДИЦИНА УНИВЕРСИТЕТІ****КАЗАХСКИЙ НАЦИОНАЛЬНЫЙ МЕДИЦИНСКИЙ УНИВЕРСИТЕТ ИМЕНИ С.Д. АСФЕНДИЯРОВА** **ASFENDIYAROV KAZAKH NATIONAL MEDICAL UNIVERSITY**  | C:\Documents and Settings\Администратор\Рабочий стол\777\logo_fin.jpg |
| Документация СМК | Утвержденоприказом Ректора |
| № приказа | Дата утверждения |
|  |  |
| Наименование документа | **Правила обеспечения непрерывности ИТ-сервисов** |
| Редакция  | 1 | Статус |
| Код  |  |  Утвержден  Рассмотрен  Отправлен на доработку  Отклонен  Другое  |
| Ответственное должностное лицо  | **Сенбеков М.Т.**Исполнительный проректор |
| Должностное лицо ‑ инициатор документа | **Каленова Б.С.**Руководитель Департамента информационных технологий |
| Предыдущий устаревший документ |  |
| Язык документа | Казахский * Русский

Английский |

Алматы‑ 2018

**ЛИСТ СОГЛАСОВАНИЯ**

|  |  |  |
| --- | --- | --- |
| Должность | Подпись | ФИО |
| Разработано: |  |  |
| Руководитель Управления программного обеспечения и телекоммуникаций |  | Зарубаев Р.Х. |
| Согласовано: |  |  |
| Исполнительный проректор |  | Сенбеков М.Т. |
| Руководитель департамента развития человеческих ресурсов и правового обеспечения |  | Аубакиров Б.Ж. |
| И.о. руководителя управления правового обеспечения |  | Богатырева Л.Б. |
| Руководитель Департамента информационных технологий |  | Каленова Б.С. |
| Руководитель отдела СМК |  | Уралова Д.Б. |

СОДЕРЖАНИЕ

[1. Общие положения 4](#_Toc511217740)

[2. Область применения 4](#_Toc511217741)

[3. Цели 4](#_Toc511217742)

[4. Термины, определения и сокращения 4](#_Toc511217743)

[5. Управление ИТ-активами 5](#_Toc511217744)

[6. Техническая поддержка ИТ-сервисов 7](#_Toc511217745)

[7. Резервное копирование и восстановление 9](#_Toc511217746)

[8. Антивирусный контроль 10](#_Toc511217747)

[9. Заключительные положения 11](#_Toc511217748)

 Лист регистрации изменений 12

 Лист ознакомления 13

# Общие положения

## Настоящие правила обеспечения непрерывности ИТ-сервисов (далее ‑ Правила) определяют основные требования к системе управления информационными технологиями Республиканского государственного предприятия на праве хозяйственного ведения «Казахский национальный университет имени С.Д. Асфендиярова» (далее ‑ Университет).

## Ознакомление с Правилами производится при приеме на работу работников, задействованных в процессе эксплуатации и обслуживании ИТ-инфраструктуры и информационных ресурсов его непосредственным руководителем.

# Область применения

## 3) Настоящие правила обязательны для применения всеми сотрудниками, задействованными в процессе управления ИТ-инфраструктурой и информационными ресурсами Университета, а также в обеспечении технической поддержки пользователей средств вычислительной техники.

# Цели

## 4) Повышение доступности информационных ресурсов и управляемости ИТ-инфраструктуры, а также обеспечения качественного оказания ИТ-услуг путем организации эффективного управления комплексом информационных технологий Университета.

# Термины, определения и сокращения

## **ИТ-сервис, ИТ-услуга** ‑ это процесс обеспечения пользователей ресурсами комплекса информационных технологий для выполнения ими своих бизнес функций.

## **Пользователь** ‑ лицо, участвующее в функционировании информационных ресурсов или использующее результаты их функционирования.

## **Средства вычислительной техники, СВТ** ‑ совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем, включая персональные компьютеры, рабочие станции, ноутбуки, серверное и сетевое оборудование, а также установленное на них программное обеспечение.

**Информационные ресурсы** ‑ информационные системы Университета, другие электронные ресурсы, в том числе доступные в них документы и информация, а также доступ к сети Интернет.

## **Локальная вычислительная сеть, ЛВС** ‑ компьютерная сеть, построенная на технологиях Ethernet, объединяющая между собой персональные компьютеры, сетевую оргтехнику, серверное и телекоммуникационное оборудование Университета.

## **Периферийные устройства** ‑ компьютерное оборудование, предназначенное для ввода/вывода информации, в том числе: монитор, клавиатура, мышь, принтер, сканер, веб-камера, акустическая система и др.

## **ИТ-инфраструктура** ‑ комплекс информационных технологий, состоящий из средств вычислительной техники, локальных вычислительных сетей, обеспечивающих работу информационных ресурсов.

## **ИТ-актив** ‑ аппаратные и программные элементы ИТ-инфраструктуры, информационные ресурсы.

## **Событие** ‑ изменение состояния ИТ-актива, которое имеет значения для управления ИТ-активом или ИТ-услугой.

## **Инцидент** ‑ незапланированное прерывание ИТ-услуг или снижение их качества, а также сбой компонентов ИТ-актива, который еще не повлиял на ИТ-услугу (например, выход из строя одного из дисков зеркального массива).

## **Работник технической поддержки** – сотрудник Университета, отвечающий за реализацию практических мероприятий по обеспечению непрерывности работы ИТ-активов и восстановлению их работы.

**ПК** ‑ персональный компьютер.

**ПО** ‑ программное обеспечение.

**ИС** ‑ Информационная система.

# Управление ИТ-активами

## 5) Для обеспечения качественного уровня ИТ-услуг и повышения уровня зрелости ИТ-инфраструктуры непосредственное участие в процессе выработки требований к приобретаемым средствам вычислительной техники, телекоммуникационного оборудования и программного обеспечения принимает Департамент информационных технологий.

## 6) При определении требований к ИТ-активам рекомендуется придерживаться следующих требований:

### Аппаратные характеристики рабочих станций и/или терминальных систем соответствуют, либо превосходят системные требования, рекомендуемые разработчиком используемого ПО.

### Характеристики серверного оборудования и систем хранения данных учитывают перспективы развития ИС и предусматривают:

#### возможность масштабирования ресурсов и увеличения производительности;

#### возможность горячей замены вентиляторов, блоков питания, дисков и адаптеров ввода-вывода;

#### систему оповещения о критических событиях;

#### средства мониторинга состояния критичных компонентов и измерения контролируемых показателей;

#### поддержку современных технологий виртуализации.

### характеристики телекоммуникационного оборудования обеспечивают базовый уровень обеспечения информационной безопасности и управляемости ЛВС.

### системное программное обеспечение приобретается с учетом:

#### соответствия требованиям, предъявляемым в техническом задании на разработку/развитие ИС или задание на проектирование;

#### соответствие типу операционных систем (клиентской или серверной);

#### совместимость с используемым прикладным ПО;

#### поддержка сетевых сервисов, функционирующих в ЛВС Университета;

#### приоритета модели лицензирования, обеспечивающей снижение стоимости закупки, а также совокупной стоимости лицензии за период эксплуатации;

#### приоритета унификации видов используемого системного ПО;

## 7) Обеспечивается достаточная полнота сведений об эксплуатируемых средствах вычислительной техники, телекоммуникационного оборудования и других элементов ЛВС, а также используемого программного обеспечения и информационных систем Университета для повышения управляемости ИТ-инфраструктуры и повышения качества ИТ-услуг.

### Управление аппаратными ИТ-активами включает в себя:

#### идентификацию, классификацию и маркировку ИТ-активов;

#### инвентаризацию и паспортизацию средств вычислительной техники, телекоммуникационного оборудования с проверкой их конфигурации;

#### своевременную актуализацию сведений об объектах ИТ-инфраструктуры при изменении их конфигурации, расположения или других значимых параметров;

#### обеспечение доступности сведений по ИТ-активам в пределах компетенции персонала Университета, задействованного в их обслуживании.

### Управление программными ИТ-активами включает в себя:

#### учет установленного программного обеспечения;

#### учет имеющихся лицензий (прав на использование) ПО;

#### контроль обновлений системного ПО.

## 8) Автоматизация процесса учета сведений об ИТ-активах и оперативного реагирования производится путем внедрения и использования систем мониторинга.

## 9) В целях контроля обновлений системного ПО обеспечивается внедрение и использование средств централизованного управления распространением обновлений системного ПО.

## 10) Все подразделения, являющиеся владельцами электронных информационных ресурсов и Интернет-ресурсов Университета, обеспечивают ведение каталога электронных информационных ресурсов[[1]](#footnote-1) и его поддержку в актуальном состоянии.

## 11) Использование доменных имен Интернет-ресурсов Университета обеспечивается владельцами Интернет-ресурсов в соответствии с Правилами регистрации, пользования и распределения доменных имен в пространстве казахстанского сегмента Интернета[[2]](#footnote-2).

## 12) Аппаратные ИТ-активы размещаются с учетом требований по снижению риска несанкционированного доступа к ним, а также подлежат защите от отказов системы электроснабжения и сбоев в работе коммунальных служб.

# Техническая поддержка ИТ-сервисов

## 13) Техническая поддержка информационных технологий обеспечивается путем применения современных подходов к управлению ИТ-услугами. Применяются следующие процессы эксплуатации:

#### Мониторинг событий ‑ раннее обнаружение инцидентов, своевременное определение необходимости обновления или масштабирования ресурсов.

#### Управление проблемами и инцидентами ‑ оперативное восстановление работоспособности ИТ-сервисов, определение времени разрешения инцидентов, категорирование инцидентов, стандартизация процесса управления инцидентами, проведение профилактических работ по предупреждению инцидентов или минимизации их влияния на ИТ-сервис.

#### Выполнение запросов на обслуживание ‑ разрешение прочих обращений пользователей, поступающих в техническую поддержку (например, запросы на смену пароля, установку ПО и другие).

#### Управление доступом ‑ предоставление легитимным пользователям прав доступа к ИТ-сервисам и управление правами доступа.

## 14) Для каждого инцидента и проблемы производится их категорирование и определяется приоритет на основе срочности решения инцидента и его влияния на деятельность Университета.

## 15) По степени влияния на деятельность Университета инциденты подразделяются на следующие категории:

### Инциденты, оказывающие малое влияние на работу ИТ-сервисов, затрагивающие одного или несущественное количество рядовых пользователей имеют средний, низкий или минимальный приоритет, который определяется исходя из срочности их решения.

### Инциденты, оказывающие среднее влияние на работу ИТ-сервисов имеют высокий, средний или низкий приоритет в зависимости от срочности их решения и определяются:

#### влиянием на работу большого количества пользователей;

#### влиянием на работу приоритетных пользователей;

#### неработоспособностью отдельных подсистем;

#### увеличением риска выхода из строя ИТ-активов при утрате работоспособности отдельных элементов, не оказавших влияние на работоспособность ИТ-сервисов.

### 15.3. Значительные инциденты, оказывающие высокое влияние на доступность ИТ-сервисов и имеют максимальный приоритет. К ним относятся:

#### выход из строя ИТ-активов, приводящий к полной неработоспособности критичных ИТ-сервисов;

#### программные и аппаратные сбои, приводящие к уничтожению, неправомерной модификации или компрометации наиболее важной информации.

## 16) Обеспечение непрерывной работы ИТ-сервисов достигается путем разработки, применения и поддержания в актуальном состоянии Плана обеспечения непрерывности и восстановления работы ИТ-активов, а также применения/проведения следующих мероприятий:

### регламентация процессов мониторинга событий, обработки инцидентов и запросов на обслуживание, а также действий работников технической поддержки по разрешению типовых инцидентов;

### подготовка работников технической поддержки;

### применение различных способов резервного копирования ИТ-активов;

### контроль над соблюдением требований по обеспечению непрерывной работы ИТ-активов;

### проведение анализа эффективности принятых мер обеспечения непрерывной работы ИТ-активов, выработка и реализация предложений по их совершенствованию.

## 17) План обеспечения непрерывности и восстановления работы ИТ-активов определяет:

#### перечень и характеристику ИТ-активов, требующих обеспечения непрерывности работы;

#### требования по восстановлению работы ИТ-активов, допустимое время неработоспособности ИТ-активов и время на их восстановление;

#### порядок действий при обнаружении нарушения непрерывной работы ИТ-активов и порядок оповещения ответственных работников;

#### порядок действий по восстановлению работы ИТ-активов;

#### порядок действий по выявлению и устранению причин нарушения работы ИТ-активов;

#### графики проведения планово-профилактических процедур по обслуживанию ИТ-активов и резервному копированию информации.

## 18) Пользователи средств вычислительной техники и информационных систем в обязательном порядке информируются о способах обращения в техническую поддержку.

#  Резервное копирование и восстановление

## 19) Процедура резервного копирования выполняется для всех баз данных информационных систем и ресурсов Университета, а также конфигураций телекоммуникационного оборудования и настроек критически значимого программного обеспечения ИТ-сервисов.

## 20) Ответственность за резервное копирование информации, хранящаяся на локальных дисках персональных компьютеров работников Университета возлагается на самих работников. В случае утраты информации ее восстановление работниками технической поддержки не гарантируется.

## 21) Расписание резервного копирования определяется для каждого ИТ-сервиса индивидуально, при этом учитывается следующее:

### Резервное копирование баз данных критичных ИТ-сервисов осуществляется не реже одного раза в сутки;

### Резервное копирование баз данных других ИТ-сервисов и прочих ресурсов производится не реже одного раза в месяц;

### Резервное копирование конфигураций телекоммуникационного оборудования и настроек критически значимого программного обеспечения производится после каждого изменения конфигурации.

## 22) При организации резервного копирования информации применяются доступные средства автоматизации процесса. Все резервные копии длительного хранения проходят процедуру проверки.

## 23) Хранение резервных копий осуществляется на отдельных носителях информации, при этом учитывается следующее:

### Хранение резервных копий баз данных критичных ИТ-сервисов осуществляется исходя из возможности восстановления информации:

#### не менее чем за предыдущие 5 (пять) лет, по состоянию на последний день года;

#### не менее чем за предыдущие 12 (двенадцать) месяцев, по состоянию на последний день месяца;

#### не менее чем за предыдущие 30 (тридцать) дней на любой момент времени.

### Хранение резервных копий баз данных прочих ИТ-сервисов и ресурсов, а также конфигураций телекоммуникационного оборудования и значимого программного обеспечения производится исходя из потребности в восстановлении, при этом обеспечивается хранение не менее 3 (трех) резервных копий.

## 24) Восстановление информации из резервных копий производится после согласования с уполномоченными на то подразделениями и/или ответственными должностными лицами и с обязательным уведомлением пользователей.

#  Антивирусный контроль

## 25) В целях обеспечения устойчивого функционирования ИТ-активов Университета и снижения риска утраты, утечки, искажения и уничтожения информации от деструктивного воздействия компьютерных вирусов и иных вредоносных программ применяется антивирусное ПО.

## 26) Антивирусное ПО устанавливается на каждой рабочей станции независимо от ее подключения к сети Университета.

### Устанавливается только последняя версия антивирусного ПО. В случае выявления сбоев в работе последней версии ПО на СВТ определенного типа, допускается установка предыдущих версий.

### Установленное антивирусное ПО должно быть настроено на автоматический запуск основных программных модулей, обеспечивающих защиту от проникновения компьютерных вирусов.

## 27) Пользователи обязаны использовать только распространяемое работниками технической поддержки антивирусное ПО.

## 28) Для защиты рабочих станций и файловых серверов Университета используется антивирусное ПО, соответствующее следующим требованиям:

### Наличие сетевого центра управления антивирусной безопасностью, который обеспечивает:

#### тиражирование клиентской части антивирусного ПО на рабочие станции и сервера Университета;

#### применение единых политик антивирусной защиты;

#### мониторинг общей защищенности сети и формирование отчетности;

### Наличие в клиентской части антивирусного ПО модулей, осуществляющих:

#### проверку на наличие вредоносного ПО до открытия файлов или запуска программ;

#### выявление подозрительной активности программ;

#### автоматическое сканирование

#### Наличие файлового сканера, запуск которого происходит по расписанию с возможностью выбора объектов сканирования.

## 29) Политика антивирусной защиты, применяемая для рабочих станций должна предусматривать наличие парольной защиты, препятствующей несанкционированному удалению или модификации настроек антивирусного ПО.

## 30) Антивирусное ПО для отдельных типов серверов (межсетевой экран, сетевой шлюз, сервисы электронной почты и пр.) может не иметь сетевого центра управления антивирусной безопасностью.

## 31) Решение о выборе антивирусного ПО принимается Департаментом информационных технологий.

#  Заключительные положения

## 32) Департамент информационных технологий несет ответственность в пределах компетенции:

#### за разработку и исполнение инструкций по идентификации, классификации и маркировки ИТ-активов Университета;

#### за актуализацию сведений об ИТ-активах Университета;

#### за разработку и исполнение Плана обеспечения непрерывности и восстановления ИТ-активов;

#### за разработку и исполнение инструкций, регламентов и другой документации к процессу управления эксплуатацией ИТ-сервисов;

#### мониторинг состояния средств антивирусного контроля.

## 33) Ответственность за обеспечение непрерывной работы, резервного копирования и восстановления электронных информационных ресурсов, Интернет-ресурсов и сервисов несут подразделения, являющиеся их владельцами.

## 34) Несоблюдение требований Правил влечет ответственность в соответствии с действующим законодательством Республики Казахстан и внутренними нормативными документами Университета.

## 35) Настоящие Правила вступают в силу после их утверждения и должны быть доведены до всех руководителей подразделений Университета, являющихся владельцами информационных систем, электронных информационных и Интернет ресурсов, а также работников, задействованных в управлении и поддержке ИТ-инфраструктуры, информационных систем и сервисов.

**ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| № п/п | Номера листов | Основание для внесения изменений | Подпись | Ф.И.О.  | Дата | Дата введения изменения |
| Замененных | Новых | Аннулированных |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

**ЛИСТ ОЗНАКОМЛЕНИЯ**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **№ п/п** | **ФИО** | **ДОЛЖНОСТЬ** | **ДАТА** | **ПОДПИСЬ** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

1. См. Единые требования в области информационно-коммуникационных технологий и обеспечения информационной безопасности, утвержденные постановлением Правительства РК от 20.12.2016 г. №832 (Глава 3, параграф 1) [↑](#footnote-ref-1)
2. Утверждены приказом министра оборонной и аэрокосмической промышленности РК от 13.03.2018 г. № 38/НҚ [↑](#footnote-ref-2)