НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы»

BU
BAITURSYNULY UNIVERSITY

Утверждаю
Председатель Правления – Ректор
_____ С.Куанышбаев
16.06 2026 г.

ПРАВИЛА

ОРГАНИЗАЦИЯ ФИЗИЧЕСКОЙ ЗАЩИТЫ, БЕЗОПАСНОЙ СРЕДЫ ФУНКЦИОНИРОВАНИЯ И ОБЕСПЕЧЕНИЯ НЕПРЕРЫВНОЙ РАБОТЫ АКТИВОВ, СВЯЗАННЫХ СО СРЕДСТВАМИ ОБРАБОТКИ ИНФОРМАЦИИ

ПР 016-2026

Костанай

Предисловие

1 РАЗРАБОТАНЫ отделом разработки и сопровождения программного обеспечения

2 ВНЕСЕНЫ отделом разработки и сопровождения программного обеспечения

3 УТВЕРЖДЕНЫ И ВВЕДЕНЫ В ДЕЙСТВИЕ: приказом Председателя Правления - Ректора от 16. 06. 2026 года № 213 ОД

4 РАЗРАБОТЧИК:
В. Гриднева – начальник отдела разработки и сопровождения программного обеспечения;

5 ЭКСПЕРТЫ:
А. Шмит – начальник отдела технического обеспечения;
В. Петрович – начальник финансово-экономической службы.

6 ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 3 года

7 ВВЕДЕНЫ впервые

Содержание

Глава 1. Область применения

1. Настоящие Правила организации физической защиты, безопасной среды функционирования и обеспечения непрерывной работы активов, связанных со средствами обработки информации (далее - Правила), регламентируют порядок организации физической защиты средств обработки информации, обеспечения их непрерывного функционирования и восстановления после инцидентов и сбоев в НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы» (далее – Университет).

2. Правила входят в состав нормативно-справочной документации Университета, являются обязательными для исполнения всеми сотрудниками Университета, а также доводятся до сведения иных третьих лиц, участвующих в эксплуатации и обслуживании средств обработки информации Университета.

Глава 2. Нормативные ссылки

3. В настоящих Правилах использованы ссылки на следующие нормативные документы:

1) Закон Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;

2) Постановление Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»;

3) Устав НАО «Костанайский региональный Университет имени Ахмет Байтұрсынұлы», утвержденный приказом Председателя Комитета государственного имущества и приватизации Министерства финансов Республики Казахстан от 05 июня 2020 года № 350 с изменениями от 03.10.2023г.;

4) СО 002-2025 Стандарт организации. Делопроизводство;

5) ДП 001-2025 Документированная процедура. Управление документацией;

6) П 054-2024 Политика информационной безопасности НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы»;

7) ПР 128-2025 Методика оценки рисков информационной безопасности НАО «Костанайский региональный университет имени Ахмет Байтұрсынұлы».

Глава 3. Определения

4. В настоящих Правилах применяются следующие определения:

1) активы, связанные со средствами обработки информации в части информационной безопасности (далее – активы ИБ) - материальный или нематериальный объект, который является информацией или содержит информацию, или служит для обработки, хранения, передачи информации и имеет ценность для Университета в интересах достижения целей и непрерывности его деятельности;

2) центр обработки данных – технологическое помещение, предназначенное для размещения серверного оборудования информационных систем Университета, а также обеспечения условий для его безопасного и бесперебойного функционирования;

3) серверное оборудование – совокупность серверов, систем хранения данных, сетевого и телекоммуникационного оборудования, обеспечивающих функционирование информационных систем Университета.

4) информационная система – под информационными системами в настоящих Правилах понимаются все информационные системы, корпоративные сервисы и веб-ресурсы Университета, используемые для обработки, хранения и передачи информации;

5) администратор информационных систем – специалист, ответственный за администрирование, сопровождение и обеспечение бесперебойного функционирования аппаратно-программного комплекса серверной инфраструктуры Университета;

6) база данных – структурированная совокупность данных, предназначенная для хранения, поиска, обработки и использования информации в рамках конкретной информационной системы Университета;

7) система управления базами данных – программное обеспечение, обеспечивающее создание, хранение, доступ, управление, обработку, защиту, резервирование и восстановление баз данных Университета.

Глава 4. Обозначения и сокращения

5. В настоящей документированной процедуре применяются следующие сокращения:

1) ДП – документированная процедура;
2) НАО – Некоммерческое акционерное общество;
3) ОДО – отдел документационного обеспечения;
4) СО – стандарт организации;
5) ИБ – информационная безопасность;
6) ИС – информационная система;
7) СУБД – система управления базами данных;
8) ЦОД – центр обработки данных;
9) ОС – операционная система;
10) П – положение;
11) ПР – правила;
12) VLAN (Virtual Local Area Network) – виртуальная локальная вычислительная сеть;
13) CPU (Central Processing Unit) – центральный процессор;
14) RAM (Random Access Memory) – оперативная память;
15) SIEM (Security Information and Event Management) – система управления событиями и информацией безопасности;

16) RAID (Redundant Array of Independent Disks) – массив независимых дисков с избыточностью.

Глава 5. Размещение серверного оборудования и порядок физического доступа

6. Серверное оборудование Университета размещается в ЦОД оператора, предоставляющего услуги по размещению оборудования (colocation), на основании заключаемого договора оказания услуг.

7. Инфраструктура ЦОД должна соответствовать требованиям Параграфа 8 «Требования к системам бесперебойного функционирования технических средств и информационной безопасности, а также серверным помещениям (ЦОД)» Постановления Правительства Республики Казахстан от 20 декабря 2016 года № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности».

8. Университет осуществляет контроль за размещением, эксплуатацией и безопасностью принадлежащего ему серверного оборудования, размещённого в ЦОД оператора, включая учёт установленного оборудования, мониторинг его состояния, организацию и контроль работ по техническому обслуживанию и модернизации, а также согласование физического доступа с оператором ЦОД.

9. При размещении серверного оборудования Университет выбирает ЦОД с учётом соблюдения следующих технологических требований:

1) снижение воздействия внешней среды на оборудование (отсутствие окон в помещениях, изоляция оборудования в гермозонах, экранирование стен);

2) минимизация риска затопления (шкафы и стойки с оборудованием размещаются на фальшполе, в помещении отсутствуют трубы водоснабжения и отопления, устанавливаются датчики затопления и системы аварийного водоотведения);

3) обеспечение гарантированного защищённого электропитания (два ввода электроснабжения от разных подстанций, электрогенераторы с автоматическим вводом резерва, источники бесперебойного электропитания, дублирование указанных систем, молниезащита и защитное заземление);

4) соблюдение требований к температуре и влажности воздуха (дублированные системы кондиционирования с автоматической ротацией основных и резервных систем);

5) соблюдение требований противопожарной безопасности (использование негорючих материалов и материалов, не поддерживающих горение, пожарно-охранная сигнализация, автоматическая система газового пожаротушения, системы дымоудаления);

6) ограничение неавторизованного доступа (помещение не является проходным, не используется для иных целей, оснащено усиленными дверьми и автоматическими управляемыми запорными устройствами);

7) наличие охранных систем (охранная сигнализация с датчиками движения и проникновения с выводом на пост охраны, система видеонаблюдения), а также аварийного освещения и щитов аварийного отключения оборудования, расположенных у выходов из помещения;

8) организация регулярного обслуживания инженерных систем;

9) разделение силовых и слаботочных кабельных систем;

10) обеспечение доступа серверного оборудования Университета к каналам связи через инфраструктуру ЦОД в соответствии с условиями договора.

11) выполнение маркировки кабелей, оборудования и серверных шкафов.

10. В целях обеспечения ИБ, сохранности серверного оборудования и бесперебойного функционирования ИС Университета физический доступ в ЦОД осуществляется исключительно для выполнения регламентированных работ.

11. Работы, требующие физического доступа в серверное помещение, выполняются администраторами ИС. Перечень указанных работ приведён в таблице 1.

12. Физический доступ сотрудников Университета в ЦОД осуществляется на основании утверждённого перечня сотрудников, допущенных к работам, требующим физического доступа к серверному оборудованию, а также официального письма на имя администрации ЦОД в соответствии с установленным оператором ЦОД пропускным режимом.

13. Посещение ЦОД осуществляется не только при возникновении инцидентов или неисправностей, но также в целях проведения плановых осмотров, проверки комплектности оборудования и выполнения диагностических мероприятий.

14. Физический доступ в ЦОД разрешен только в рабочее время. В нерабочее время доступ возможен только в экстренных случаях.

Таблица 1 – Перечень работ, требующих физического доступа в ЦОД

№ п/п	Наименование работ	Описание
1	2	3
1	Работы по перезапуску и аварийному отключению оборудования	Перезагрузка, принудительное выключение или включение серверного и сетевого оборудования в случаях, когда удалённое администрирование невозможно
2	Работы по техническому обслуживанию и контролю состояния оборудования	Диагностика, плановые осмотры и профилактические работы, проверка комплектности и состояния оборудования, визуальный контроль условий размещения и эксплуатации, очистка оборудования, а также ремонт и замена комплектующих при необходимости.

1	2	3
3	Работы по модернизации и установке оборудования	Установка, демонтаж, перемещение серверного и сетевого оборудования, монтаж кабельной инфраструктуры
4	Устранение внештатных ситуаций	Действия при отказе оборудования, нарушении соединений
5	Работы сотрудников сторонних организаций	Работы по гарантийному обслуживанию, ремонту оборудования, выполнению договорных обязательств при обязательном сопровождении уполномоченного сотрудника Университета

Глава 6. Удаленный доступ

15. Под удаленным доступом к серверам Университета подразумевается регламентированный доступ через корпоративную сеть Университета к серверам информационных систем (ИС).

16. В таблице 2 представлен перечень работ, требующих удаленного доступа к серверному оборудованию.

Таблица 2. Перечень работ, требующих удаленного доступа к серверному оборудованию

№ п/п	Наименование работ	Описание
1	2	3
1	Работы по эксплуатации и сопровождению серверной инфраструктуры и системного ПО	1) Обеспечение функционирования серверного оборудования и ОС; 2) Настройка и оптимизация производительности; 3) Обновление серверного программного обеспечения, СУБД; 4) Управление ресурсами и дисковым пространством; 5) Резервное копирование и восстановление ОС и баз данных; 6) Анализ системных журналов и предупреждение сбоев. 7) Контроль корректности резервного копирования и восстановления; 8) Общий контроль состояния серверной инфраструктуры.

1	2	3
2	Работы по администрированию сетевой инфраструктуры	1) Мониторинг состояния сетевого оборудования (коммутаторы, маршрутизаторы, межсетевые экраны); 2) Анализ и устранение сетевых сбоев; 3) Настройка VLAN, маршрутизации и сетевых сервисов; 4) Управление правилами межсетевого экранирования; 5) Обновление прошивок сетевого оборудования; 6) Резервное копирование и восстановление конфигураций; 7) Мониторинг сетевой нагрузки и выявление аномалий; 8) Анализ сетевых инцидентов ИБ.
3	Работы по контролю функционирования информационных систем	1) Проверка корректности функционирования ИС и веб-приложений; 2) Обновление ИС; 3) Контроль состояния серверных ресурсов (включая дисковое пространство); 4) Выявление сбоев и нарушений в работе ИС.
4	Работы по внедрению и развитию новых информационных систем	1) Установка и первичная настройка ИС; 2) Развертывание новых сервисов и приложений; 3) Тестирование и ввод в эксплуатацию; 4) Миграция и интеграция ИС.
5	Работы по администрированию систем виртуализации	1) Управление гипервизорами и виртуальными машинами; 2) Создание, настройка и удаление виртуальных машин; 3) Мониторинг ресурсов (CPU, RAM); 4) Обеспечение отказоустойчивости; 5) Резервное копирование и восстановление виртуальных сред; 6) Обновление платформ виртуализации; 7) Контроль безопасности виртуальной инфраструктуры.

1	2	3
6	Работы по администрированию систем хранения данных	1) Управление системами хранения; 2) Настройка RAID, томов и пулов хранения; 3) Мониторинг состояния дисков и контроллеров; 4) Обеспечение отказоустойчивости хранения данных; 5) Резервное копирование и восстановление данных.
7	Работы по обеспечению информационной безопасности и мониторингу	1) Мониторинг событий ИБ; 2) Анализ журналов безопасности; 3) Выявление и реагирование на инциденты; 4) Управление средствами защиты (антивирус, SIEM и др.); 5) Контроль уязвимостей и обновление систем безопасности; 6) Проведение проверок и аудита безопасности.

17. Все работы выполняются администратором ИС Университета.

18. Все работы по удалённому доступу к серверам Университета должны выполняться с использованием безопасных протоколов и фиксироваться в журналах событий информационной системы, если таковые предусмотрены используемой системой.

Глава 7. Техническое обслуживание серверного оборудования

19. В Университете осуществляется надлежащее техническое обслуживание серверного оборудования для обеспечения его непрерывной работоспособности, целостности и надежности функционирования. В этих целях применяются следующие мероприятия:

1) оборудование обслуживается не реже раз в год;

2) техническое обслуживание и ремонт оборудования выполняются администратором ИС Университета или специалистами, допущенными к работе с серверным оборудованием;

3) при вывозе серверного оборудования за пределы ЦОД или университета для проведения ремонта и технического обслуживания сторонними организациями носители информации (диски) подлежат изъятию либо обеспечивается защита данных с использованием средств шифрования;

4) накопители информации при списании оборудования подлежат обязательной очистке от данных безопасным способом, а в случае невозможности очистки - физическому уничтожению.

20. Все работы по техническому обслуживанию серверного оборудования,

устранению неисправностей, а также восстановлению работоспособности оборудования и программного обеспечения подлежат обязательному документированию путем ведения журнала технического сопровождения оборудования, в котором фиксируются сведения о выполненных работах, сбоях и отказах, а также результатах восстановительных мероприятий.

Глава 8. Порядок идентификации причин прерывания процессов функционирования активов информационной безопасности и обеспечения непрерывности их функционирования

21. Сотрудники, ответственные за обеспечение ИБ Университета идентифицируют причины прерывания работы ИС и активов ИБ на основе результатов работ, выполненных в соответствии с ПР 128-2025. Методика оценки рисков информационной безопасности.

22. Сотрудники, ответственные за обеспечение ИБ Университета на основе результатов оценки рисков ИБ определяют угрозы и последствия идентифицированных причин прерывания работы ИС и активов ИБ с учетом возможного ущерба и времени восстановления.

23. Сотрудники, ответственные за обеспечение ИБ Университета составляют перечень требований по обеспечению непрерывной работы ИС Университета согласно указанной форме таблицы 3.

Таблица 3. Форма перечня требований информационных систем университета, подлежащих обеспечению непрерывной работы

№	Наименование информационной системы	Время работы информационной системы	Минимальное допустимое время восстановления случаев сбоя информационной системы	Максимальное допустимое время восстановления случаев сбоя информационной системы	Наиболее благоприятные дни для проведения технических работ
1	2	3	4	5	6

24. Для обеспечения непрерывной работы и правильной эксплуатации ИС Университета сотрудниками отдела разработки и сопровождения программного обеспечения разрабатываются эксплуатационные документы (инструкции) для каждой ИС Университета. В эксплуатационных документах указываются:

1) назначение и назначенные функции ИС;
2) поставщик и версия системы, если она приобретена;
3) порядок установки и настройки (для собственных установок – описание действий, выполненных Университетом; для готовых систем – ссылка на официальную документацию поставщика);
4) регламентируемые действия при сбоях или некорректной работе, включая восстановление из резервной копии и порядок обращения к поставщику

или ответственному сотруднику;

5) ответственные лица за эксплуатацию и сопровождение ИС.

25. Сотрудники, ответственные за обеспечение ИБ и администраторы ИС не реже одного раза в год проводят анализ эффективности мер по защите активов ИБ от отказов, сбоев и иных нарушений функционирования, а также разрабатывают и реализуют мероприятия по их предупреждению и минимизации последствий.

Глава 9. Ответственность

26. Администраторы ИС несут персональную ответственность за все действия, совершенные в ЦОД и удаленно.

27. Руководство университета обеспечивает выделение необходимых ресурсов, включая финансирование, для приобретения, внедрения, эксплуатации и защиты активов ИБ, включая серверное оборудование и иные средства обработки информации.

Глава 10. Порядок внесения изменений

28. Внесение изменений в настоящие Правила осуществляется по инициативе начальника отдела разработки и сопровождения программного обеспечения, начальника отдела технического обеспечения, проректором по исследованиям, инновациям и цифровизации в соответствии с ДП 001-2025 Документированная процедура. Управление документацией.

Глава 11. Согласование, хранение и рассылка

29. Согласование и рассылка Правил производятся в соответствии с ДП 001-2025 Документированная процедура. Управление документацией.

30. Настоящие Правила согласовываются с проректором по исследованиям, инновациям и цифровизации, начальником отдела правового обеспечения и государственных закупок, начальником отдела управления персоналом и начальником отдела документационного обеспечения.

31. Подлинник настоящих Правил вместе с «Листом согласования» передается на хранение в ОДО по акту приема-передачи.

32. Рабочий экземпляр настоящих Правил размещается на сайте Университета с доступом из внутренней корпоративной сети.