«УТВЕРЖДЕНО»
Решением Правления
НАО «Университет Нархоз»
Протокол №____от
«___»._____.20___ г.

Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов в Некоммерческом акционерном обществе «Университет Нархоз»

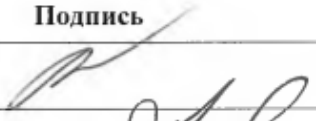
Алматы, 2023

Оглавление

Паспорт документа

Наименование документа:	Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов в Некоммерческом акционерном обществе «Университет Нархоз»
Краткое описание:	Правила организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов в Некоммерческом акционерном обществе «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	Бисенғали Л	
Советник по цифровизации	Тебаев Д.Б.	
и.о. Директора Департамента информационных технологий	Жумажанов Б.Ж.	

1 **Общие положения**

1.1 Настоящие Правила физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов в Некоммерческом акционерном обществе «Университет Нархоз» (далее – «Правила») определяют порядок по организации физической защиты средств обработки информации и безопасной среды функционирования информационных ресурсов Некоммерческого акционерного общества «Университет Нархоз» (далее – «Общество»).

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».

3 **Размещение и защита оборудования**

3.1 Оборудование должно быть расположено и защищено так, чтобы уменьшить риск от воздействий окружающей среды и возможности неавторизованного доступа.

3.2 Необходимо рассматривать следующие мероприятия по управлению информационной безопасностью:

- оборудование необходимо размещать таким образом, чтобы свести до минимума излишний доступ в места его расположения;
- средства обработки и хранения важной информации следует размещать так, чтобы, уменьшить риск несанкционированного наблюдения за их функционированием;
- отдельные элементы оборудования, требующие специальной защиты, необходимо изолировать, чтобы повысить общий уровень необходимой защиты;
- меры по управлению информационной безопасностью должны свести к минимуму риск потенциальных угроз, например, воровство, пожар, взрыв, задымление, затопление (или перебои в подаче воды), пыль, вибрация, химические воздействия, помехи в электроснабжении, помехи связи, электромагнитное облучение, вандализм;
- следует проводить мониторинг состояния окружающей среды в целях выявления условий (температура, влажность), которые могли бы неблагоприятно повлиять на функционирование средств обработки информации;
- все здания должны быть оснащены громоотводами, а все внешние линии связи оборудованы специальными грозозащитными фильтрами;
- следует использовать специальные средства защиты, оборудования, расположенного в производственных цехах, например, защитные пленки для клавиатуры;
- оборудование для обработки важной информации должно быть защищено с целью свести к минимуму риск по утечке информации, вследствие электромагнитного излучения.

3.3 Оборудование необходимо защищать от перебоев в подаче электроэнергии и других

сбоев, связанных с отказами в обеспечении вспомогательных услуг.

3.4 Все вспомогательные услуги, такие как электричество, водоснабжение, канализация, отопление, вентиляция и кондиционирование, должны соответствовать системам, для которых они предназначены. Все инженерные системы и их оборудования должны регулярно осматриваться и соответствующим образом тестироваться для обеспечения их надлежащего функционирования и сокращения риска вследствие их неисправности или сбоя.

3.5 Также необходимо обеспечить подходящее энергоснабжение, соответствующее техническим характеристикам от производителя оборудования.

3.6 Чтобы обеспечить безопасное выключение и/или непрерывное функционирование устройств, поддерживающих критические бизнес-процессы, необходимо подключать оборудование через UPS. Резервный генератор следует применять, если необходимо обеспечить функционирование оборудования в случае длительного отказа подачи электроэнергии от общего источника. Для бесперебойной работы генератора в течение длительного срока необходимо обеспечить соответствующую поставку топлива. Оборудование UPS и генераторы следует регулярно проверять на наличие адекватной мощности, а также тестировать в соответствии с рекомендациями производителя.

3.7 Аварийные выключатели электропитания необходимо располагать около запасных выходов помещений, где расположено оборудование, чтобы ускорить отключение электропитания в случае критических ситуаций. Следует обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети.

3.8 Система водоснабжения должна быть стабильной и приемлемой для обеспечения кондиционирования воздуха, увлажнения воздуха (при необходимости) и оборудования систем пожаротушения.

3.9 Телекоммуникационное оборудование должно быть подключено к системным поставщикам, по крайне мере двумя разными маршрутами, чтобы предотвратить отказ одного канала подключения услуги телефонии. Услуги телефонии должны удовлетворять и соответствовать нормативным требованиям аварийной связи.

3.10 Силовые и телекоммуникационные кабельные сети, к которым передаются данные или осуществляются другие информационные услуги, необходимо защищать от перехвата информации или повреждения.

3.11 Необходимо рассматривать следующие мероприятия:

- силовые и телекоммуникационные линии, связывающие средства обработки информации, должны быть, по возможности, подземными или обладать адекватной альтернативной защитой;
- сетевой кабель должен быть защищен от неавторизованных подключений или повреждения, например, посредством использования специального кожуха или выбора маршрутов прокладки кабеля в обход общедоступных участков;
- силовые кабели должны быть отделены от коммуникационных, чтобы исключить помехи;
- четко определенная маркировка кабелей и оборудования должна быть использована для минимизации обработки ошибки, такие как неправильно выбранные сетевые кабели.

4 **Физический доступ**

4.1 Правила доступа в помещения Общества

4.1.1 Доступ работников в здание размещения Общества, производится в соответствии с принятыми правила пропускного и внутри объектного режима.

4.1.2 В производственное здание Общества организован один основной вход:

- Для поддержания порядка в вестибюле дежурит охранник; Работники Общества должны пользоваться служебным входом, где размещается основной пост контроля, где

проходит регистрация времени прихода и ухода работников посредством Face ID, а также регистрация выдачи и приема ключей от служебных кабинетов.

4.1.3 Если посетителю необходимо пройти в здание, он должен обратиться на пост контроля со стороны служебного входа и по внутреннему телефону известить необходимого ему работника о своем приходе. Посетитель проходит в здание с представителем структурного подразделения, в чьих услугах он нуждается, или может пройти самостоятельно после телефонного указания охраннику от работника пропустить данного посетителя. В обоих случаях охранник регистрирует посетителя в журнале.

4.1.4 Работники службы охраны круглосуточно обеспечивают контроль по предотвращению внештатных ситуаций, возможных в связи с прорывом сетей, нарушением электроснабжения и др.

4.1.5 Доступ в помещения Общества, осуществляется на основе системы контроля доступа, включающей в себя следующие элементы: ключи от кабинетов, охранная сигнализация, пост охраны здания.

4.2 Доступ к серверному оборудованию

4.2.1 Под физическим доступом к серверам и кроссовым Общества подразумевается доступ к непосредственному физическому контакту с серверным оборудованием.

4.2.2 Основные сервера находятся в Дата-центре и резервный в серверной комнате. В дата-центре обеспечены все необходимые условия для работы серверного оборудования и организованы процедуры контроля доступа во все помещения.

4.2.3 Доступ в серверное помещение, где располагается серверное оборудование Общества, осуществляется согласно действующим требованиям

4.2.4 В случае необходимости доступа в серверное помещение лицам, не входящим в список администраторов информационных ресурсов Общества, оформляется заявка с обоснованием причин необходимости доступа. При наличии разрешительного документа, администратора информационных ресурсов должен сопровождать лиц, которым разрешен доступ в серверное помещение.

4.2.5 За нарушение пропускного режима виновные сотрудники привлекаются к дисциплинарной ответственности, предусмотренной действующим законодательством Республики Казахстан.

5 **Перечень работ, требующих физического доступа к серверам**

5.1 Администраторы информационных ресурсов в серверном помещении проводят работы согласно таблице 1.

Таблица 1 – Перечень работ, требующих физического доступа к серверам

№ п/п	Наименование работ	Описание	Ответственные за выполнение	Обоснование для физического доступа
1	Перезагрузка сервера	Выполняется нажатием кнопки Reset на сервере	Администратор информационных ресурсов	Невозможность выполнения перезагрузки удаленно
2	Работы по техническому обслуживанию серверов	Ремонт, замена, установка, переустановка оборудования, профилактические работы.	Администратор информационных ресурсов	Техническое обслуживание серверов невозможна без прямого доступа к ним

3	Работы обслуживающего персонала	Уборка серверного помещения	Администратор информационных ресурсов/ сотрудники дата центра	Для уборки серверного помещения необходим прямой доступ в серверное помещение
4	Устранение внештатных ситуаций	Сбои и отключение электропитания, отсоединения соединительных проводов и коммуникаций, пожары, наводнения и д.р.	Администратор информационных ресурсов, СУБД, ППО/ сотрудники дата центра	Для устранения внештатных ситуаций необходим прямой доступ в серверное помещение
5	Работы сотрудников сторонних организаций	Переустановка, обновление прикладного ПО	Администратор информационных ресурсов, ППО	Для переустановки и обновления прикладного ПО необходим прямой доступ к серверу

6 **Удаленный доступ**

6.1 Под удаленным доступом к серверам информационных ресурсов Общества подразумевается регламентированный доступ через корпоративную сеть Общества.

6.2 Перечень работ требующих удаленного доступа к серверам.

В таблице 2 представлен перечень работ, требующих удаленного доступа к серверам.

Таблица 2 – Перечень работ, требующих удаленного доступа к серверам

№ п/п	**Наименование работ**	**Описание**	**Ответственные за выполнение**
	Работы по администрированию	– Проверка целостности файловой системы; – Управление безопасностью ОС; – Мониторинг производительности и настройка ОС; – Управление дисковым пространством; – Резервное копирование ОС; – Работы по остановке и запуску приложений в случае сбоя и т.д.	Администратор информационных ресурсов
		– Управление пространством БД; – Управление приложениями и кодом; – Управление резервированием восстановлением БД; – Управление системными ресурсами;	Администратор СУБД

		– Управление безопасностью СУБД; – Обновление версии СУБД.	
		– Управление и разработка приложения, а также работы по остановке и запуску приложений в случае сбоя.	Администратор ППО

7 **Техническое обслуживание оборудования**

7.1 В Обществе должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и целостности.

В этих целях следует применять следующие мероприятия:

- оборудование следует обслуживать в соответствии с инструкциями и периодичностью, рекомендуемыми поставщиком;
- необходимо, чтобы техническое обслуживание и ремонт оборудования проводились только авторизованным персоналом;
- следует хранить записи обо всех предполагаемых или фактических неисправностей и всех видах профилактического и восстановительного технического обслуживания;
- необходимо принимать соответствующие меры безопасности при отправке оборудования для технического обслуживания за пределы организации в отношении удаленных, стертых и перезаписанных данных.

8 **Безопасная утилизация (списание) или повторное использование оборудования**

8.1 Все компоненты оборудования, содержащего носители данных следует проверять на предмет удаления всех важных данных и лицензионного программного обеспечения.

8.2 Носители данных, содержащие важную информацию, необходимо физически разрушать или перезаписывать безопасным образом, а не использовать стандартные функции удаления.

8.3 В отношении носителей данных, содержащих важную информацию, может потребоваться оценка рисков с целью определения целесообразности их разрушения, восстановления или выбраковки.

9 **Внос/вынос оборудования**

9.1 Оборудование, информацию или программное обеспечение можно выносить из помещений организации только на основании соответствующего разрешения.

Следует рассматривать следующие мероприятия:

- оборудование, информация или программное обеспечение не должны вывозиться за пределы организации без соответствующего разрешения.
- должны быть четко определены права на вывоз активов за пределы помещений сотрудниками, подрядчиками или пользователями сторонних организаций;
- необходимо установить лимит времени для вывоза оборудования и соблюдения условий возврата;
- оборудование следует регистрировать при выносе и при вносе, а также делать отметку, когда оно возвращено в журнале регистрации согласно Приложению 1 к настоящим Правилам.

10 **Ответственность**

10.1 Работники, имеющие доступ к серверному оборудованию, несут ответственность за:

- за надлежащее выполнение своих функциональных обязанностей;
- за сохранность, доступность, конфиденциальность обрабатываемой информации, в рамках своей компетенции.

10.2 Уполномоченные работники или подрядная организация, действующая на основании договора, несут ответственность за регулярное проведение проверок работоспособности источников бесперебойного питания и генератора.

10.3 Директор ДИТ или лицо его заменяющее несет ответственность за согласование разрешения на доступ в серверные помещения.

10.4 Пользователи информационных ресурсов Общества несут ответственность за своевременное информирование соответствующих лиц об известных им фактах и событиях, свидетельствующих о нарушении порядка обеспечения физической безопасности.

10.5 Выполнение требований настоящих Правил контролирует ответственный по ИБ.

11. Заключительные положения

11.1. Настоящие Правила утверждаются решением Правления.

11.2. Изменения и дополнения в Правила вносятся решением Правления.

Приложение 1

Форма журнала учета вноса/выноса оборудования

п/п	**ФИО работника**	**Описание оборудования, основание для вноса/выноса**	**Дата**	**Подпись работника**	**Ответственный**

ЛИСТ ОЗНАКОМЛЕНИЯ

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