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

Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации информационных систем и IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»

Алматы, 2023

Оглавление

Паспорт документа

Наименование документа:	Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации информационных систем и IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Краткое описание:	Правила идентификации, классификации и маркировки активов, связанных со средствами обработки информации информационных систем и IT инфраструктуры Некоммерческого акционерного общества «Университет Нархоз»
Тема:	Информационная безопасность
Статус:	Новый
Дата утверждения:	«___» _____2023г.
Дата завершения действия:	
Дата аудита:	Ежегодно
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 идентификации, классификации и маркировки активов, связанных со средствами обработки информации информационных систем и IT инфраструктуры НАО «Университет Нархоз» (далее – «инфраструктура НАО «Университет Нархоз») некоммерческого акционерного общества «Университет Нархоз» (далее – Правила) разработаны в соответствии с требованиями законодательства и стандарта Республики Казахстан, стандартом информационной безопасности ТОО «Verny Capital» VC 04.04.2022 внутренними актами НАО «Университет Нархоз».

1.2 Правила определяют основные меры, методы и порядок идентификации, классификации и маркировки активов и программно-аппаратных средств инфраструктура НАО «Университет Нархоз», а также способы и средства идентификации, классификации активов информационных систем или/и основных компонентов информационных системы, а также программно-аппаратных средств информационных системы. Кроме того, Правила описывают порядок маркировки активов в зависимости от их установленного класса, конфиденциальности, ценности и критичности.

1.3 Целью настоящих Правил является обеспечение соответствующей защиты активов, связанных со средствами обработки информации.

1.4 В настоящих Правилах используются следующие основные термины и определения:

- **Актив** – все, что имеет ценность для инфраструктуры НАО «Университет Нархоз»;
- **Активы программного обеспечения** – прикладное программное обеспечение, системное программное обеспечение, инструментальные средства разработки и утилиты;
- **Владелец актива** – лицо, подразделение или учреждение, на которого возложена ответственность по контролю за разработкой, поддержкой, использованию и безопасности активов;
- **Информационные активы** – информация и данные в любом виде, получаемые, хранимые, обрабатываемые, передаваемые, оглашаемые, в том числе базы данных, системная документация, руководства пользователя, учётные материалы, процедуры эксплуатации, планы по обеспечению непрерывности функционирования информационного обеспечения и другая документация;
- **Некоммерческое акционерное общество (НАО)** – Некоммерческое акционерное общество «Университет Нархоз»;
- **Персонал** – пользователи, работники, администраторы;
- **Реестр активов** – систематизированный перечень активов Общества;
- **Специалист, ответственный за информационную безопасность (далее – Ответственный за ИБ Общества)** – работник Общества, в должностные обязанности которого входит обеспечение ИБ;
- **Физические активы** – программное обеспечение независимо от формы получения (приобретённое, собственной разработки, свободно распространяемые), компьютерное, серверное и телекоммуникационное оборудование, оборудование связи, печатная техника, магнитные носители и другие технические средства;
- **Услуги** – вычислительные услуги, услуги связи и другие услуги;

1.5 Актуальность идентификационной информации активов обеспечивается Ответственным за ИБ Общества.

1.6 После проведения процедуры идентификации активов, заполняется Реестр активов (далее – Реестр) инфраструктуры НАО «Университет Нархоз», по форме согласно Приложению 1 к Правилам, который хранится для свода и учета.

2 **Ссылки**

2.1 Настоящий документ разработан 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 **Порядок проведения идентификации, классификации и маркировки активов**

3.1 Общество должно идентифицировать все активы и документировать важность этих активов. Инвентаризация активов должна включать всю информацию, необходимую для восстановления активов после какого-либо бедствия, включая тип актива, формат, местоположение, дублирующую информацию, информацию о лицензиях и ценность бизнеса. Инвентаризация не должна без необходимости дублировать другие инвентаризации, а должна обеспечивать корректировку своего содержания. Вся информация на активы, связанные со средствами обработки информации, должны быть в собственности Общества.

3.2 Идентификация заключается в проведении инвентаризации и составлении реестра активов инфраструктуры НАО «Университет Нархоз»

3.3 По итогам работ идентификации активов, для каждого актива дается оценка его ценности.

Ценность актива определяется исходя из ущерба, который будет нанесен инфраструктуре НАО «Университет Нархоз» в случае потери активом его свойств безопасности с нарушением конфиденциальности, целостности и доступности информационных активов или иных установленных требований, а также исходя от стоимости создания и обслуживания актива.

3.4 Для определения ценности актива и маркировки используются следующие уровни:

- **«высокий»** (3) уровень подразумевает, что в результате потери свойств безопасности актива, Обществу будет нанесен значительный ущерб;
- **«средний»** (2) уровень подразумевает, что в результате потери свойств безопасности актива, Обществу будет нанесен существенный ущерб;
- **«низкий»** (1) уровень подразумевает, что в результате потери свойств безопасности актива, Обществу будет нанесен незначительный ущерб.

3.5 По результатам оценки, активы в Реестре должны быть размещены и сортированы по значимости, наиболее значимые активы должны располагаться в начале Реестра.

3.6 Каждый актив, вносимый в Реестр активов, подлежит описанию и это описание должно содержать информацию в отношении:

- наименования актива;
- идентификатора актива, в случае наличия (тип актива, серийный номер или инвентарный номер);
- владельца актива;
- физического или логического месторасположения актива;
- ценности актива (по конфиденциальности, целостности и доступности).

3.7 Каждому активу, внесенному в Реестр активов, присваивается уникальный инвентарный номер.

3.8 Допускается проведение процедур конфигурирования и внесения актуальной информации в Реестр активов Ответственным за ИБ Общества, о чем делается соответствующая пометка в Реестре активов. Актуализация информации, представленной в обозначенном Реестре, осуществляется Владельцем актива.

3.9 Для обеспечения защиты активов, связанных со средствами обработки информации необходимо:

- определить категории активов (таблица 1);
- провести инвентаризацию активов;
- классифицировать активы.

В Обществе определены следующие категории активов:

Таблица 1 – Категории активов

№ категории	Наименование	Описание
1	Информационные активы	– базы данных и файлы данных, системная документация, резервные копии; – руководства пользователя, учетные материалы, процедуры эксплуатации или поддержки; – (обслуживания), планы по обеспечению непрерывности функционирования; – информационного обеспечения, процедуры действий при сбоях, архивированная информация.
2	Активы программного обеспечения	– прикладное программное обеспечение, системное программное обеспечение; – инструментальные средства разработки и утилиты.
3	Физические активы	– серверное оборудование, рабочие станции, магнитные диски (CD-носители); – телекоммуникационное оборудование и другое техническое оборудование.
4	Услуги	вычислительные услуги и услуги связи, основные коммунальные услуги, например, отопление, освещение, электроэнергия, кондиционирование.
5	Персонал	квалификация, навыки и опыт.
6	Нематериальные активы	престиж (имидж) владельца и собственника информационной системы.

3.10 В соответствии с вышеприведенной категорией активов должна проводиться их идентификация и инвентаризация, данные которых записываются в реестр. Актуализация данных реестра должна проводиться соответствующим владельцем актива не реже 1 раза в год. Проверка реестра на актуальность содержащихся в нем данных проводится Ответственным за ИБ Общества во время проведения аудитов ИБ.

4 **Маркировка активов по конфиденциальности, ценности и критичности**

4.1 Информационные активы поделены и маркируются Владельцами активов по следующей классификации:

- информация, открытая для доступа (открытая информация);
- информация с ограниченным доступом - конфиденциальная (доступ к которым ограничен законами Республики Казахстан, либо их собственником или владельцем, в случаях, установленных законодательством Республики Казахстан).

Конфиденциальная информация включает в себя:

– информация для внутреннего использования – внутренняя информация;

– персональные данные.

4.2 Принципы категорирования информации, предоставления доступа и передачи информации приведены в таблицах 2 и 3.

Таблица 2 – Принципы категорирования информации

Классификация информации	**Принципы категорирования**	**Принципы предоставления доступа, хранения и передачи информации**
Открытая	Информация, разрешенная к открытому опубликованию, ее разглашение не оказывает негативного влияния на деятельность Общества. Такая информация может передаваться за пределы Общества, в том числе в СМИ.	Доступ к информации могут иметь все сотрудники.
Информация для внутреннего пользования	Информация, разглашение которой оказывает негативное влияние на деятельность Общества, либо носит локальный характер, а также внутренняя информация, доступ к которой не ограничен, но обращение и порядок предоставления которой регламентированы Обществом, как собственником (владельцем) информации.	Доступ к информации предоставляется только при наличии производственной необходимости. Производственная необходимость должна быть подтверждена в письменной форме. Правом предоставления и лишения доступа к информации обладает её владелец или уполномоченное им лицо. Информация может быть передана за пределы Общества с письменного разрешения Владельца актива. В данную категорию входят все виды неклассифицированной информации, по которой не принято решение о разрешении ее передачи.
Персональные данные	Сведения, относящиеся к определенному или определяемому на их основании субъекту персональных данных, зафиксированные на электронном, бумажном и(или) ином материальном носителе; Информация, разглашение которой оказывает негативное влияние на деятельность Общества.	Доступ к информационным ресурсам, содержащим общедоступные персональные данные, является свободным с согласия субъекта персональных данных или на которые в соответствии с законами Республики Казахстан не распространяются требования соблюдения конфиденциальности. Доступ к информационным ресурсам, содержащим персональные данные ограниченного доступа, ограничен субъектом персональных данных или законами Республики Казахстан. При передаче ПД через сеть необходимо применять технологии шифрования или при взаимодействии с третьими сторонами применять обезличивание данных. За незаконный сбор и обработку персональных данных, касающихся частной жизни физических

		лиц, должностные лица несут ответственность, предусмотренную законами Республики Казахстан.

Таблица 3 – Принципы предоставления доступа и передачи информации

Категория	**Действия**	**Меры безопасности**
Открытая информация	Маркировка:	Допустимо отсутствие маркировки.
	Хранение:	Свободное хранение.
	Передача:	Свободная передача.
	Обсуждение:	Свободное обсуждение.
Внутренняя информация	Маркировка:	Маркируется грифом «Внутренняя информация».
	Хранение:	**Съемные носители, бумажные копии** – в местах специального хранения, запираемых на ключ. **Электронные копии** – на ноутбуках или персональных компьютерах и серверах.
	Передача:	**Электронная почта –** передача в пределах организации или между организациями. **Печать –** на принтер в пределах контролируемой зоны с немедленным изъятием распечаток. **Съемные носители, бумажные копии –** внешняя доставка – курьером в запечатанных конвертах; с пометкой – «Вскрывать только получателем».
	Уничтожение:	**Бумажные копии** – с помощью шредера, **электронные копии** - удаление файлов.
	Обсуждение:	При проведении совещаний, аудио - и видеоконференций, организатор конференции утверждает список участников. **Телефон** – не рекомендуется использование средств связи сторонних операторов, домашних телефонов.
Персональные данные	Маркировка:	Маркируется грифом «Персональные данные».
	Хранение:	**Бумажные носители** – в сейфе (ячейке металлического шкафа с надежными запорными устройствами). **Электронные копии** - зашифрованное хранение.
	Передача:	В зашифрованном виде.

	Уничтожение:	Экспертной комиссией любым способом, исключающим ознакомление посторонних лиц.
	Обсуждение	Обсуждение по телефону – только после идентификации другой стороны, но не рекомендуется.

5 **Порядок ведения реестра активов**

5.1. Маркировка активов в зависимости от их установленного класса, конфиденциальности, ценности и критичности производится при составлении реестра активов.

5.2. Реестр активов, связанных со средствами обработки информации, должен содержать данные о:

- Классе актива:

– программное обеспечение;

– аппаратное средство;

– активы телекоммуникационного обеспечения;

– информационные активы.

- Виде актива:

– вид программного обеспечения;

– вид аппаратного средства;

– вид телекоммуникационного средства;

– вид информации общего и ограниченного доступа.

- Значимость актива (расставление значимости от «1» до «5», где «1» - наивысшая степень значимости, «5» наименьшая. Либо «Незначительная», «Существенная» или «Критическая».) Оценка активов осуществляется в соответствии с Методикой оценки рисков.

5.3 Рекомендуется включать в реестр активов информацию по физическому или логическому местонахождению актива.

Маркировка активов, связанных со средствами обработки информации состоит из нескольких этапов:

- категорирование всех видов информации, используемой при решении задач на конкретных компьютерах (установка категорий класса, конфиденциальности, ценности и критичности конкретных видов информации);
- категорирование активов, связанных со средствами обработки информации, которые имеются в Обществе;
- исходя из максимальных категорий обрабатываемой информации устанавливается категория актива, связанного со средствами обработки информации.

Необходимо использовать форму маркировки активов достаточную для:

- идентификации класса актива;
- идентификации вида актива;
- идентификации ценности актива (значимости);
- идентификации владельцев актива, группы активов.

Необходима физическая маркировка активов, при невозможности, как в случае с информационными активами, то допускается применения электронных аналогов маркировки.

Таблица 4 – Классификация активов

п/п	Класс актива	Вид актива	Ценность актива/группы Кф+Цл+Дт	Владелец
			Кф – Конфиденциальность Цл – Целостность Дт – Доступность	

По результатам оценки, активы в Реестре должны быть размещены и сортированы по значимости, наиболее значимые активы должны располагаться в начале Реестра согласно форме Таблицы 4.

6 **Ответственность**

6.1. Владелец актива несет ответственность за полноту и достоверность внесенных в Реестр сведений.

6.2. Владелец актива несет ответственность за определение классификации актива, периодический пересмотр и обеспечивает ее постоянное обновление.

6.3. Ответственный за ИБ Общества несет ответственность за периодический пересмотр и актуализацию реестра.

7 Заключительные положения

7.1. Правила утверждаются решением Правления.

7.2. Изменения и дополнения в Правила утверждаются решением Правления.

Приложение 1 к правилам идентификации, классификации и маркировки активов, связанных со средствами обработки информации инфраструктуры НАО «Университет Нархоз»»

Реестр активов

№	Название	Идентификатор актива (если есть)	Владелец	Описание	Требование по			Тип актива	Представление	Местоположение
					конфиденциальности	целостности	доступности			
1	2	3	4	5	6	7	8	9	10	11

ЛИСТ ОЗНАКОМЛЕНИЯ

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