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

Политика информационной безопасности Некоммерческого акционерного общества «Университет Нархоз»

Алматы, 2023

Оглавление

Паспорт документа

Наименование документа:	Политика информационной безопасности Некоммерческого акционерного общества «Университет Нархоз»
Краткое описание:	Политика информационной безопасности 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 Настоящая Политика информационной безопасности некоммерческого акционерного общества «Университет Нархоз» (далее – «Политика») разработана в соответствии с законодательством Республики Казахстан, требованиями международных стандартов управления информационной безопасностью, стандартом по информационной безопасности ТОО «Verny Capital», Уставом и иными внутренними документами Некоммерческого акционерного общества «Университет Нархоз» (далее – «Общество»).

1.2 Политика определяет основные принципы, направления и требования по защите информации, является основой для обеспечения режима информационной безопасности.

1.3 Цель Политики – обеспечение и защиты объектов IT инфраструктуры, автоматизированных информационных систем Общества от возможного нанесения ей материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация уровня рисков.

1.4 Основными задачами Политики являются:

1) надлежащая защита от неправомерного использования информации ограниченного распространения, банковской, коммерческой и других видов тайн, иной конфиденциальной информации, отнесенной к таковой Положением об определении информации об некоммерческом акционерном обществе «Университет Нархоз», или его деятельности, составляющей служебную, коммерческую или иную охраняемую законом тайну, а также порядок ее раскрытия;

2) прогнозирование и своевременное выявление угроз безопасности информационным ресурсам Общества, причин и условий, способствующих нанесению финансового, материального ущерба, нарушению их нормального функционирования и развития;

3) создание условий функционирования Общества с наименьшей вероятностью реализации угроз безопасности информационных ресурсов и нанесения ущерба;

4) создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявление негативных тенденций в функционировании Общества, на основе нормативных, правовых, организационных и технических мер и средств обеспечения безопасности;

5) создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями физических и (или) юридических лиц.

1.5 Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информации и (или) поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является Общество.

1.6 Положения настоящей Политики относятся ко всем штатным работникам и временным работникам, имеющим доступ к автоматизированным и телекоммуникационным системам Общества.

1.7 Неотъемлемой частью организации защиты информации является непрерывный контроль эффективности предпринимаемых мер, определение для работников Общества перечня недопустимых действий, возможных последствий и ответственности.

2 **Термины и определения**

2.1 В настоящей Политике используются следующие термины:

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищенность информации от ее нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного ее тиражирования.

Доступность – возможность для авторизованного пользователя автоматизированной информационной системы за приемлемое время получить информационную услугу, предусмотренную функциональностью.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информационная безопасность – комплекс административно-правовых, организационно-распорядительных и технических мер, направленные на обеспечение конфиденциальности, целостности и санкционированной доступности информации в процессе ее сбора, обработки, передачи и хранения.

Конфиденциальность – защита от несанкционированного ознакомления.

Несанкционированное действие – действие субъекта в нарушение установленных в системе правил обработки информации.

Пользователь – субъект, пользующийся информацией, полученной от ее собственника, владельца или посредника в соответствии с установленными правами и правилами доступа к информации.

Сеть (локальная сеть, ЛВС, LAN) – группа точек, узлов или других устройств, соединенных коммуникационным набором оборудования, обеспечивающих соединение станций и передачу между ними информации.

Риски информационной безопасности – реально или потенциально возможные действия по реализации опасных воздействующих факторов с целью преднамеренного или случайного нарушения режима функционирования объекта.

Уязвимость – любая характеристика автоматизированной системы, использование которой может привести к реализации угроз.

Целостность информации – свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому ее состоянию).

Шифрование – преобразование данных в нечитабельную форму, используя ключи шифрования-расшифровки.

3 **Принципы информационной политики**

3.1 Основными принципами построения системы обеспечения безопасности информации Общества и ее функционирования являются:

1) **законность** – соблюдение законодательства по защите информации и законных интересов всех участников информационного обмена;

2) **системность** – подход к вопросам организации информационной безопасности должен быть логическим и последовательным: в первую очередь оценка риска информационной безопасности исходя из реальных угроз и уязвимости информационных ресурсов, затем создание комплекса организационных и технических мер и средств защиты, учитывающих специфику Общества;

3) **эффективность** – реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению информационной безопасности должны сводить риски к минимуму, при этом адекватность и эффективность защитных мер должна быть оцениваема на регулярной основе;

4) **целесообразность** – соблюдение соразмерности затрат на обеспечение защиты информации и потенциальных потерь при реализации угроз;

5) **непрерывность** – принцип функционирования системы информационной безопасности, обеспечивающий непрерывную работу технических и программных средств, а также включающий меры по постоянному контролю системы информационной безопасности;

6) **взаимодействие и координация** – осуществление мер обеспечения информационной безопасности на основе четкой взаимосвязи подразделения, в функции которого входит

обеспечение функционирования IT инфраструктуры и информационных систем Общества и подразделений-пользователей информационных ресурсов, сторонних специализированных организаций в области защиты информации и обслуживания информационных систем, координации их усилий для достижения поставленных целей, а также взаимодействия с с иными заинтересованными органами;

7) **совершенствование** – совершенствование мер и средств защиты информации на основе собственного опыта, появления новых технических средств с учетом изменений в методах и средствах атак информационных ресурсов, нормативно-технических требований, достигнутого отечественного и зарубежного опыта;

8) **приоритетность** – категорирование (ранжирование) всех информационных ресурсов Общества по степени важности и оценка реальных, а также потенциальных угроз информационной безопасности;

9) **информированность и персональная ответственность** – пользователи информационных ресурсов должны знать о наличии системы контроля и защиты информации, информационные сервисы индивидуально идентифицируют пользователей и инициируемые ими процессы;

10) **соответствие стандартам** – система информационной безопасности соответствует международным стандартам в данной области;

11) **обязательность контроля** – контроль за деятельностью пользователей, а также мониторинг IT инфраструктуры должен осуществляться на основе применения средств оперативного контроля и регистрации, охватывать как несанкционированные, так и санкционированные действия.

4 **Ответственность и обязательства руководства**

Эффективная безопасность требует подотчетности, исчерпывающего определения и признания обязанностей в сфере безопасности. Руководство должно отвечать за все аспекты управления безопасностью, включая принятие решений по управлению рисками. Отдельные ее факторы, такие как тип, форма регистрации, размер и структура общества, повлияют на то, на каком уровне будут определены эти обязанности. Руководство принимает непосредственное участие в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности общества, законами и нормативными актами.

Руководство осуществляет поддержку заданного уровня информационной безопасности путем внедрения системы менеджмента, а также путем распределения обязанностей и ответственности персонала за ее обеспечение (приказ о назначении ответственных лиц, должностные инструкции и т.д.).

Руководство обязано:

1. формулировать, пересматривать и утверждать политику информационной безопасности, а также следить за эффективностью реализации политики информационной безопасности;

2. обеспечивать четкое управление и реальную поддержку инициатив в области информационной безопасности;

3. предоставлять ресурсы для обеспечения информационной безопасности;

4. обеспечивать координацию мер контроля информационной безопасностью в организации;

5. утверждать роли и обязанности сотрудников по информационной безопасности общества посредствам должностных инструкций, приказов, указов и т.д.;

6. инициировать идеи, планы и программы по поддержанию осведомлённости об информационной безопасности, определять потребность обучения пользователей и администраторов методам и процедурам обеспечения безопасности, определять обязанности, относящиеся к установке и обслуживанию программного обеспечения и аппаратной части;

7. обеспечивать проведение испытаний программных продуктов и аппаратных средств

информационных систем перед вводом в промышленную эксплуатацию, все требования должны быть определены документально;

8. определять потребность в консультации специалиста внутри организации или со стороны по вопросам информационной безопасности, просматривать и координировать результаты консультации по всей организации;

9. четко устанавливать ответственность руководителей подразделений за различные активы и процессы безопасности, детали этой ответственности должны быть документированы, уровни полномочий должны быть ясно определены и документированы (акт о материальной ответственности);

10. ведение практики дисциплинарного взыскания в случае нарушения Политики информационной безопасности;

11. ликвидации последствий нарушения информационной безопасности;

12. обязательность и своевременность выявления, пресечение попыток нарушения установленных правил обеспечения информационной безопасности. Контроль деятельности пользователей, каждого средства зашиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации.

Работники должны быть ознакомлены с мерами ответственности за разглашение информации в соответствии с их функциональными обязанностями, а также с мерами ответственности за возможные нарушения.

Обслуживающий персонал IT инфраструктуры при нарушении требований пунктов политики ИБ будет привлекаться к административной или иной ответственности, в соответствии с действующим законодательством Республики Казахстан.

5 **Объекты обеспечения информационной безопасности**

5.1 Основными объектами обеспечения информационной безопасности в Обществе признаются следующие элементы:

1) информационные ресурсы, содержащие сведения, отнесенные в соответствии с действующим законодательством к коммерческой тайне Общества, а также информацию, необходимую для обеспечения нормального функционирования Общества (в дальнейшем – защищаемая информация);

2) технические средства и системы информатизации (персональные компьютеры, серверы, сети и др.), на которых производится обработка, передача и хранение защищаемой информации;

3) программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение) IT инфраструктуры Общества, с помощью которых производится обработка защищаемой информации;

4) помещения, предназначенные для ведения закрытых переговоров и совещаний;

5) помещения, в которых расположены средства обработки защищаемой информации.

5.2 Подлежащая защите информация может:

1) находиться на бумажных носителях;

2) находиться в электронном виде (храниться, обрабатываться и передаваться);

3) передаваться по телефону, телефаксу, телексу и т.п. в виде электрических сигналов;

4) передаваться в устном виде во время совещаний и переговоров;

5) записываться и воспроизводиться с помощью технических средств (диктофоны, видеомагнитофоны и др.).

6 **Меры обеспечения безопасности**

6.1 Меры обеспечения безопасности компьютерных систем подразделяются на:

– правовые (законодательные);

– морально-этические;

– организационные (административные);

– физические;

– технические (аппаратные и программные).

6.2 Законодательные (правовые) меры защиты. К правовым мерам защиты относятся действующие в Республике Казахстан нормативные и правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

6.3 Организационные (административные) меры защиты. Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования системы обработки данных в Обществе, использование ее ресурсов, деятельность обслуживающего персонала информационных систем обработки данных Общества, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

6.4 Физические меры защиты. Физические меры защиты основаны на применении разного рода механических, электро- или электронно- механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам информационной системы обработки данных Общества и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

6.5 Технические (программно-аппаратные) меры защиты. Технические меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав автоматизированной информационной системы Общества и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическую защиту информации и т.д.).

7 **Риски информационной безопасности**

7.1 Под рисками информационной безопасности понимаются потенциально возможные негативные воздействия на защищаемую информацию, к числу которых относятся:

1) утрата сведений, составляющих банковскую тайну, коммерческую тайну, конфиденциальную информацию Общества и иную защищаемую информацию, а также искажение (несанкционированная модификация, подделка) такой информации;

2) утечка – несанкционированное ознакомление с защищаемой информацией посторонних лиц (несанкционированный доступ, копирование, хищение и т.д.), а также утечка информации по каналам связи и за счет побочных электромагнитных излучений;

3) недоступность информации в результате ее блокирования, сбоя оборудования или программ, дезорганизации функционирования операционных систем рабочих станций, серверов, маршрутизаторов, систем управления баз данных, распределенных вычислительных сетей, воздействия вирусов, стихийных бедствий и иных форс-мажорных обстоятельств;

4) отсутствие планирования и контроля;

5) низкая степень надежности программного обеспечения;

6) недостаточная осведомленность работников Общества (об информационной безопасности и ответственности за возможные негативные последствия за вышеперечисленные риски), низкая квалификация пользователей в области информационных технологий.

7.2 В результате воздействия указанных рисков могут возникнуть следующие негативные последствия, влияющие на состояние информационной безопасности Общества и его нормальное функционирование:

1) финансовые потери, связанные с утечкой или разглашением защищаемой информации;

2) финансовые потери, связанные с уничтожением и последующим восстановлением утраченной информации;

3) ущерб от дезорганизации деятельности Общества и потери, связанные с невозможностью выполнения им своих обязательств;

4) моральные потери (ущерб репутации Общества).

8 **Техническое обеспечение информационной безопасности Общества**

8.1 Техническое обеспечение информационной безопасности должно базироваться на:

1) системе унификации и взаимного дополнения применяемых средств защиты;

2) системе лицензирования деятельности;

3) системах сертификации или проверки всего программного обеспечения и средств защиты.

8.2 Система обеспечения безопасности информационных ресурсов должна предусматривать комплекс организационных, технических средств и мер по защите информации в процессе документооборота, при работе работников с конфиденциальными документами и сведениями, при обработке информации в автоматизированных системах различного уровня и назначения, при передаче по каналам связи, при ведении конфиденциальных переговоров.

8.3 Предоставление прав доступа специалистам Общества к соответствующей информации определяется в порядке, определяемом внутренними документами Общества.

8.4 Одним из направлений технического обеспечения информационной безопасности является защита информационных ресурсов от хищения, утраты, уничтожения, разглашения, утечки, искажения и подделки за счет несанкционированного доступа и иных воздействий.

8.5 В рамках технического обеспечения информационной безопасности предусматривается:

1) реализация единой разрешительной системы допуска работников к работам, документам и информации конфиденциального характера;

2) ограничение доступа работников и посторонних лиц в здания, помещения, где обрабатывается (хранится) информация конфиденциального характера;

3) разграничение доступа пользователей к данным автоматизированных систем различного уровня и назначения;

4) учет документов, информационных массивов, регистрация действий пользователей информационных систем, контроль за несанкционированным доступом и действиями пользователей;

5) предотвращение внедрения в автоматизированные информационные системы программ вирусного характера.

8.6 Защита информационных ресурсов от несанкционированного доступа предусматривает:

1) обеспечение безопасности автоматизированных систем, регистрации и проверки прав доступа специалистов Общества;

2) персональную ответственность работника за использование и сохранность доверенной информации (документов, носителей информации, информационных массивов), за свои действия в автоматизированной информационной системе;

3) надежность хранения информации (документов, носителей информации, информационных массивов) в условиях, исключающих несанкционированное ознакомление, ее уничтожение, подделку или искажение;

4) целостность технической и программной среды, обрабатываемой информации и средств защиты, предполагающую физическую сохранность средств информатизации, неизменность программной среды, изолированность средств защиты от пользователей.

8.7 Обеспечение безопасности информационных систем предполагает разработку необходимых мер защиты на этапе формирования будущей автоматизированной системы, что заключается в составлении спецификаций на приобретаемое оборудование и программное обеспечение с учетом предъявляемых требований по безопасности.

8.8 В процессе формирования заказа на построение информационных систем учитывается не только основной набор функциональных сервисов (системы автоматизации процедур, делопроизводства и тому подобные), но и ряд необходимых вспомогательных сервисов, обеспечивающих надежное функционирование системы и требуемый уровень безопасности. Обеспечение процедур регистрации и предоставления доступа реализуется в рамках разрешительной системы допуска к работам, документам и сведениям, которая предполагает определение для всех пользователей автоматизированных систем доступные им информационные и программные ресурсы, а также конкретные операции (чтение, запись, модификация, удаление, выполнение) с помощью заданных программно-технических средств доступа.

8.9 Система контроля за действиями работников реализуется с помощью организационных мер и технических средств контроля при работе с конфиденциальными документами и сведениями;

8.10 Целостность автоматизированных систем достигается комплексом программно-технических средств и организационных мероприятий, осуществляемых уполномоченным подразделением Общества.

8.11 Необходимой составляющей системы безопасности является обеспечение качества работ и используемых средств и мер защиты, нормативной базой которого является система стандартов и других нормативных правовых актов по безопасности.

8.12 В целях обеспечения заданного качества функционирования системы информационной безопасности, должно проводиться предпроектное обследование и проектирование IT инфраструктуры, выработка требований по средствам защиты информации и контроля, предполагаемых к использованию в этих системах, а также контроль защищенности информационных ресурсов.

8.13 Применение аутентификации в автоматизированных системах обусловлено необходимостью гарантированного сопоставления участников информационного обмена учетным записям в системе в целях защиты участников информационного обмена от стороннего вмешательства путем взаимной идентификации. Важной мерой защиты передаваемых в электронном виде данных является шифрование.

9 **Организационное обеспечение информационной безопасности**

9.1 В работе с работниками Общества основными организационными мерами в плане достижения информационной безопасности являются:

1) заключение трудовых договоров и получение у работников добровольного согласия на соблюдение требований, регламентирующих режим информационной безопасности и сохранность конфиденциальной информации;

2) проведение периодического обучения и повышения квалификации работников Общества в области информационной безопасности.

9.2 Система распределения обязанностей между отдельными работниками в значительной мере способствует повышению общего уровня информационной безопасности, что достигается разделением полномочий и дублированием контроля. В системах с высокими требованиями по обеспечению сохранности данных ответственная работа или процедура (например, изменение статуса электронного документа) выполняется после подтверждения ее необходимости двумя работниками.

9.3 Административные меры защиты информации предполагают:

1) обеспечение физической сохранности автоматизированной системы и дополнительного оборудования;

2) организацию контроля доступа и режима выполнения работ персоналом подразделения информационных технологий;

3) контроль правильности и полноты выполнения работником структурного подразделения, в функции которого входит обеспечение функционирования информационных систем, мер по обеспечению сохранности необходимых дубликатов файлов, библиотеки программ, оборудования системы;

4) практическую проверку функционирования отдельных мер защиты: предотвращения недозволенных изменений программ и оборудования, контроль всех процедур, производимых с файлами на носителях и т.д.;

5) проверку машинных и ручных протоколов выполнения работ со стороны пользователей;

6) ознакомление работников со всеми новыми разработками по обеспечению сохранности данных.

10 **Разделение полномочий и ответственность**

10.1 Руководство Общества осуществляет координацию деятельности всех структурных подразделений для организации и поддержания соответствующего уровня информационной безопасности.

10.2 Контроль нештатных ситуаций и инцидентов в области защиты информации, осуществляет специалист по информационной безопасности.

10.3 Эксперт по информационной безопасности выполняет мониторинг защищенности информационных ресурсов, программно-аппаратного комплекса, контроль и анализ эффективности мер по обеспечению информационной безопасности, контролирует соблюдение требований информационной безопасности всеми участниками информационного обмена.

10.4 Администраторы ресурсов автоматизированных информационных систем Общества обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для проведения в жизнь политики безопасности.

Задачей каждого пользователя информационных систем является соблюдение требований и рекомендаций по обеспечению безопасной работы IT инфраструктуры , извещение руководства обо всех подозрительных ситуациях при работе с информационными ресурсами.

10.6 За несоблюдение порядка и правил использования информационных ресурсов к виновным лицам могут быть применены меры, предусмотренные трудовыми договорами, заключенными между Обществом и работником, а также действующим законодательством Республики Казахстан и настоящей Политикой.

11 **Заключительные положения**

11.1 Положения политики информационной безопасности Общества требуют пересмотра и корректировки не реже одного раза в год согласно плану.

Внеплановый пересмотр Политики безопасности проводится в случае:

1) внесения существенных изменений в IT инфраструктуру;

2) изменениями в законодательстве, организационной структуре;

3) возникновения инцидентов информационной безопасности.

При внесении изменений учитываются:

1)результаты аудита информационной безопасности, а также результаты предыдущих аудитов;

2)рекомендации независимых экспертов по информационной безопасности;

3)существенные угрозы и уязвимости автоматизированной информационной системы;

4)отчеты об инцидентах в области информационной безопасности;

5)рекомендации органов государственной власти.

Пересмотр Политики осуществляется специалистами, ответственным за ее разработку, внедрение и включает оценку возможности улучшения ее положений и процесса управления информационной безопасностью в соответствии с изменениями.

11.2 Настоящая Политика подлежит обязательному пересмотру по результатам проведения анализа и оценки рисков информационной безопасности для IT инфраструктуры и должна актуализироваться по мере необходимости.

11.3 Пересмотренная политика информационной безопасности утверждается уполномоченными лицами и вступает в силу с момента ее утверждения.

11.4 Настоящая Политика утверждается решением Правления.

11.5 Изменения и дополнения в настоящую Политику вносятся решением Правления.