УТВЕРЖДЕНО
Решением Совета директоров
НАО «Южно-Казахстанский
университет им.М.Ауэзова»
(Протокол № 4 от 24 декабря2020 г.)

ПОЛОЖЕНИЕ
об информационной безопасности некоммерческого акционерного общества «Южно-Казахстанский университет им.М.Ауэзова»

Шымкент, 2020г.

Подпись корпоративного секретаря

1. Общие положения

1. Настоящее Положение об информационной безопасности некоммерческого акционерного общества «Южно-Казахстанский университет им.М.Ауэзова» (далее – Положение) разработано в соответствии с Законом Республики Казахстан «Об акционерных обществах», Уставом некоммерческого акционерного общества «Южно-Казахстанский университет имени М.Ауэзова» (далее - Общество) и определяет задачи, правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности с учетом перспектив развития корпоративной сети Общества.

2. Целью настоящего Положения является обеспечение информационной безопасности объектов защиты Общества от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, минимизация ущерба от возможной реализации угроз безопасности персональных данных.

3. Требования Положения распространяются на структурные подразделения Общества, в которых осуществляется обработка информации, в том числе информации с ограниченным распространением (служебная информация) или персональных данных, а также осуществляющих сопровождение, обслуживание и обеспечение функционирования Общества. Положение распространяется также на другие организации и учреждения, осуществляющие взаимодействие с Обществом в качестве поставщиков и потребителей (пользователей) информации и услуг.

4. За организацию и обеспечение эффективного функционирования системы защиты информации в Общества несет ответственность Департамент цифровизации (далее - ДЦ).

5. ДЦ проводит необходимые технические и организационные мероприятия для обеспечения информационной безопасности.

6. ДЦ осуществляет организацию разработки системы защиты информации и организационного обеспечения ее функционирования в Обществе.

2. Назначение, нормативная и правовая база

7. Положение действует в единой информационной телекоммуникационной среде, объединяющей информационную систему (далее – ИС) Общества.

8. Положение является методологической базой для:

1) координации деятельности структурных подразделений при проведении работ по соблюдению требований обеспечения информационной безопасности;

2) совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;

3) обеспечения информационной безопасности.

9. Нормативно-правовой базой настоящего Положения являются: Законы Республики Казахстан «О национальной безопасности Республики Казахстан», Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года», «О государственных секретах», «О противодействии терроризму», «Об электронном документе и электронной цифровой подписи», «Об информатизации», «О техническом регулировании», «О лицензировании», «О средствах массовой информации».

3. Цели и задачи

10. Основной целью является надежное обеспечение информационной безопасности и как следствие недопущение нанесения материального, физического, морального или иного ущерба Обществу в результате информационной деятельности.

11. Цель достигается посредством обеспечения и постоянного поддержания следующего состояния корпоративной сети передачи данных (далее - КСПД):

1) доступность обрабатываемой информации для зарегистрированных пользователей;

2) устойчивое функционирование КСПД Общества;

3) обеспечения конфиденциальности информации, хранимой, обрабатываемой средствами компьютерной техники (далее - СКТ) и передаваемой по каналам связи;

4) целостность и аутентичность информации, хранимой и обрабатываемой ИС Общества и передаваемой по каналам связи.

12. Для достижения поставленной цели необходимо решить следующие задачи:

1) эффективное функционирование информационных ресурсов Общества и защита от вмешательства посторонних лиц в процесс;

2) разграничение уровней доступа зарегистрированных пользователей к информации, аппаратными и программными средствами защиты, используемыми в ИС;

3) контроль целостности среды исполнения программ и ее восстановление в случае нарушения;

4) защита информации от несанкционированной модификации;

5) контроль используемых программных средств, а также защиту системы от внедрения вредоносного программного обеспечения;

6) защиту служебной тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;

7) обеспечение авторизации и аутентификации пользователей;

8) своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;

9) создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;

10) создание и обеспечения бесперебойной работы электронного документооборота.

4. Пользователи информационных систем

13. К пользователям информационных систем относятся:

1) все сотрудники Общества, обладающие основными правами и обязанностями в соответствии с законодательством Республики Казахстан;

2) вспомогательный, обслуживающий и технический персонал подведомственных и сторонних организаций, осуществляющих взаимодействие с Обществом в качестве поставщиков и потребителей информации и услуг, в том числе:

3) администраторы КСПД, ответственные за сопровождение телекоммуникационного оборудования;

4) системные администраторы, ответственные за сопровождение общего и прикладного программного обеспечения;

5) потребители услуг – лица и/или сторонние организации, использующие информационные ресурсы Общества.

6) преподаватели, студенты, магистранты и докторанты.

5. Потенциальные нарушители

14. Потенциальный нарушитель информационной безопасности рассматривается как, лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий могут реализовать разнообразные угрозы информационной безопасности, направленные на ИС и нанести моральный и/или материальный ущерб интересам Общества.

15. Потенциальных нарушителей можно разделить на внутренних и внешних.

Внутренними нарушителями могут быть сотрудники Общества и вспомогательный персонал, их можно разделить на следующие группы в зависимости от уровня доступа к информационным ресурсам корпоративной сети:

1) лица, имеющие доступ к информации, составляющую персонифицированные и служебную тайны;

2) лица, имеющие доступ к информации, составляющую служебную тайну и задействованные в технологии обработки, передачи и хранения информации;

3) лица, не имеющие доступ к информации, составляющую персонифицированные секреты и служебную тайну, но задействованные в технологии обработки, передачи и хранения информации;

4) обслуживающий персонал.

Внешними нарушителями могут быть:

1) бывшие сотрудники и вспомогательный персонал;

2) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности;

3) посетители, представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.

16. В Обществе могут иметь место следующие виды нарушений:

1) несанкционированное использование программ, негативно влияющих на работоспособность КСПД Общества, снизить ее производительность, а также мешающих корректной работе КСПД;

2) нарушения сотрудниками вследствие незнания требований информационной безопасности и внутренних нормативных документов Общества.

6. Средства и меры защиты информации

17. Защита информации от утечки по каналам их передачи из/в Обществе достигается, путем применения комплексных программных, технических средств защиты и организационных мер.

18. Для выявления утечки информации необходим систематический контроль каналов утечки и оценки их опасности в пределах контролируемой зоны.

19. Организуется система регистрации, передачи, приема и хранения носителей информации, предусматриваются способы их уничтожения, с целью исключения возможности восстановления записанных на них сведений. Технические каналы передачи информации оснащаются соответствующими средствами защиты. Создается надежная система охраны зданий и сооружений, организуется пропускной режим в помещения Общества для предотвращения доступа посторонних лиц.

7. Меры по защите средств компьютерной техники

20. Защита СКТ от несанкционированного доступа в Обществе проводится по ряду направлений, для чего создается автоматизированная регистрация пользователей, система блокирования учетных записей, проводятся организационные мероприятия по предотвращению несанкционированного доступа, в том числе в случае утраты паролей и выхода из строя СКТ.

21. В случае обнаружения фактов несанкционированного доступа к информационным ресурсам и системам Общества или выявления потенциаль-

ной угрозы информационной безопасности сотрудники ДЦ немедленно информируют Правление.

8. Защита от аппаратных спецвложений, нелегального внедрения и использования неучтенных программ

22. Для предотвращения аппаратных спецвложений используются меры физической защиты, устанавливаются средства видеонаблюдения и контроля доступа в серверное помещение Общества.

23. Для защиты от нелегального внедрения и использования неучтенных программ в Обществе устанавливается базовый комплекс программного обеспечения, который необходимо устанавливать на рабочие станции пользователей. В базовый комплекс включается лицензионное программное обеспечение, необходимое для обеспечения работоспособности СКТ.

9. Защита от несанкционированного копирования данных пользователем

24. Хранящаяся в Обществе защищаемая и обрабатываемая информация, подлежит копированию и передаче третьему лицу только с разрешения Правления по согласованию с членом Правления, курирующим данный вопрос, согласно Правил пользователя по эксплуатации средств компьютерной техники и программного обеспечения Общества.

25. Лицо, совершившее передачу и копирование защищаемой информации, без разрешения, другому лицу привлекается к дисциплинарной ответственности.

10. Защита от действий вредоносных программ, вирусов

26. Для защиты от действий вредоносных программ и вирусов в Обществе используются программные средства, защищенные от несанкционированной модификации, специальные программы-анализаторы, осуществляющие постоянный контроль отклонений в деятельности прикладных программных продуктов, проверку наличия возможных следов вирусной активности, а также контроль новых программ перед их использованием.

11. Защита от хищения носителей информации

27. Устанавливается определенный порядок хранения и использования носителей информации, согласно Правилам пользователя по эксплуатации средств компьютерной техники и программного обеспечения.

28. При передаче носителя цифровой информации для повторного использования за пределами Общества проводится его очистка с целью исключения несанкционированного разглашения защищаемых сведений.

12. Защита от ошибок программно-аппаратных средств

29. Перед вводом в эксплуатацию, программные продукты и аппаратные средства подлежат тестированию и проверке на работоспособность. Не пригодные к использованию программное обеспечение и аппаратные средства в эксплуатацию не принимаются.

13. Защита от некомпетентного использования, настройки или неправомерного отключения средств защиты

30. Защита КСПД вводимого в эксплуатацию, сопровождается и используется в соответствии с регламентом. Контроль за процессом осуществляет ДЦ, обеспечивающий информационную безопасность.

31. Сопровождением серверов Общества занимается ДЦ.

32. При нарушении регламента сотрудники привлекаются к ответственности в соответствии с законодательством Республики Казахстан.

14. Защита средств компьютерной техники от нарушений работоспособности или разрушения аппаратных, программных, информационных ресурсов

33. В результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций могут возникнуть нарушения работоспособности СКТ, а также разрушение аппаратных, программных, информационных ресурсов в Обществе. На такие случаи предусматриваются соответствующие меры защиты, согласно Плану по обеспечению непрерывной деятельности информационных систем Общества.

15. Защита от незаконного подключения к корпоративной сети передачи данных

34.Защита коммуникаций от незаконного подключения кроме средств санкционированного электронного и физического доступа, осуществляется программными, техническими средствами и организационными мерами. Проводятся необходимые мероприятия для своевременного выявления, предупреждения и пресечения неправомерных действий лиц по получению доступа к коммуникациям. За незаконное подключение и попытку незаконного подключения к линиям связи и сетевому оборудованию лица несут ответственность в соответствии с законодательством Республики Казахстан.

16. Защита от повреждения, некорректного функционирования, частичного или полного отказа сетевого оборудования

35. Повреждение, некорректное функционирование, частичный, полный отказ сетевого оборудования Общества может быть, в первую очередь, в ре-

зультате возникновения аварий, стихийных бедствий и иных внештатных ситуаций.

36.В Обществе принимаются меры, связанные с внедрением средств защиты, которые будут использоваться в случае стихийных бедствий (пожаров, наводнений и землетрясений), а также в различных нештатных ситуациях.

37. В Обществе действуют Правила обеспечения непрерывной работы и восстановления по обеспечению непрерывной деятельности информационных систем Общества.

17. Защита от неправомерного включения, выключения оборудования

38. Сетевое оборудование КСПД Общества вводится в эксплуатацию, сопровождается и используется в соответствии с установленным регламентом. Включение и отключение оборудования производится уполномоченным техническим персоналом, по согласованию с ДЦ.

18. Прочие меры по защите информации

39.В Обществе должны быть соблюдены исчерпывающие меры защиты информации на всех устройствах при передаче СКТ на ремонт сторонним организациям.

40.Соблюдение требований Положения об информационной безопасности обязательно для всех пользователей информационных систем Общества.

19. Заключение

41.Утверждение Положения, а также внесение изменений и дополнений в него осуществляется по решению Совета директоров Общества.

42. Если отдельные пункты настоящего Положения вступают в противоречие с действующим Законодательством, эти пункты утрачивают силу и в части регулируемых этими пунктами вопросов следует руководствоваться нормами действующего Законодательства и (или) Уставом Общества до момента внесения соответствующих изменений в настоящее Положение.