УТВЕРЖДЕНО
Решением Совета директоров НАО «Северо-Казахстанский университет им. М. Козыбаева» (Протокол № 4 от 24 мая 2021 года)

ПОЛОЖЕНИЕ

об информационной безопасности НАО «Северо-Казахстанский университет им. М. Козыбаева»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение учитывает современное состояние и ближайшие перспективы развития корпоративной сети передачи данных Общества, цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее ресурсов и устанавливает правила, требования и ответственность за ее нарушение.
2. Требования Положения распространяются на структурные подразделения Общества в которых осуществляется автоматизированная 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.
3. За непосредственную организацию (построение) и обеспечение эффективного функционирования системы защиты информации в Обществе отвечают: Департамент информатизации образования, юридический отдел, Департамент экономического планирования и финансов, служба управления персоналом.
4. Директор Департамента информатизации образования, руководитель юридического отдела, директор Департамента экономического планирования и финансов, руководитель службы управления персоналом проводят необходимые технические и организационные мероприятия, осуществляет организацию квалифицированной разработки (совершенствования) системы защиты информации и организационного (административного) обеспечения ее функционирования в Обществе.
5. В рамках реализации решения по информационной безопасности приказом Заместителя Председателя Правления – Ректора создается

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

рабочая группа задачами которой являются анализ и прогнозирование ситуации в области информационной безопасности, выявление рисков информационной безопасности.

2. НОРМАТИВНЫЕ ССЫЛКИ

6. Положение разработано на основании:
1) Закона Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;
2) Постановления Правительства Республики Казахстан от 14 сентября 2004 года № 965 «О некоторых мерах по обеспечению информационной безопасности в Республике Казахстан»;
3) Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 17799-2006 Методы обеспечения защиты свод правил по управлению защиты информаций;
4) Государственный стандарт Республики Казахстан СТ РК ГОСТ Р 50739-2006. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

3. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

7. В Положении использованы следующие обозначения и сокращения:
1) ДИО – Департамент информатизации образования.
2) ИС – информационная система.
3) КСПД – корпоративная сеть передачи данных.
4) НСД – несанкционированный доступ.
5) ОТС – отдел технического сопровождения.
6) ПО – программное обеспечение.
7) СВТ – средства вычислительной техники.
8) БД – база данных.

4. ЦЕЛИ И ЗАДАЧИ

8. Основной целью, на достижение которой направлены все пункты Положения, является надежное обеспечение информационной безопасности и, как следствие, недопущение нанесения материального, физического, морального или иного ущерба Обществу в результате информационной деятельности.
9. Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния КСПД:
1) доступность обрабатываемой информации для зарегистрированных пользователей;

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

2) устойчивое функционирование КСПД Общества;
3) обеспечение конфиденциальности информации, хранимой, обрабатываемой СВТ и передаваемой по каналам связи;
4) целостность и аутентичность информации, хранимой и обрабатываемой ИС Общества и передаваемой по каналам связи.

10. Для достижения поставленной цели необходимо решать следующие задачи:
1) защита от вмешательства посторонних лиц в процесс функционирования информационных ресурсов Общества;
2) разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и криптографическими средствами защиты, используемыми в ИС;
3) регистрация в системных журналах действий пользователей при использовании сетевых ресурсов;
4) периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов специалистами информационной безопасности;
5) контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
6) защита информации от несанкционированной модификации, искажения;
7) контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносного программного обеспечения;
8) защиту служебной тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;
9) обеспечение авторизации и аутентификации пользователей, участвующих в информационном обмене;
10) своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;
11) создание условий и инструкций для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;
12) создание и обеспечение бесперебойной работы электронного документооборота;
13) постоянный аудит информационной безопасности.

5. ПОЛЬЗОВАТЕЛИ ИНФОРМАЦИОННЫХ СИСТЕМ

11. К пользователям информационных систем относятся:
1) сотрудники, профессорско-преподавательский состав, осуществляющие свою деятельность в Обществе и обладающие

основными правами и обязанностями в соответствии с законодательством Республики Казахстан;

2) вспомогательный персонал - обслуживающий и технический персонал сторонних организаций, осуществляющих взаимодействие с Обществом в качестве поставщиков и потребителей (пользователей) информации и услуг. В том числе:

- администраторы корпоративной сети передачи данных, ответственные за сопровождение телекоммуникационного оборудования;
- системные администраторы, ответственные за сопровождение общего и прикладного программного обеспечения;
- разработчики прикладного программного обеспечения;
- инженеры-программисты, технические специалисты;

3) потребители услуг – лица и/или сторонние организации, использующие информационные ресурсы Общества;

4) студенты, интерны, магистранты и докторанты.

6. МОДЕЛИ ПОТЕНЦИАЛЬНЫХ НАРУШИТЕЛЕЙ

12. В качестве потенциального нарушителя информационной безопасности рассматривается 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 информационные ресурсы и нанести моральный и/или материальный ущерб интересам Общества.

13. Потенциальных нарушителей делятся на внутренних и внешних. К внутренним нарушителям относятся все сотрудники Общества и вспомогательный персонал. Их делят на следующие группы в зависимости от уровня доступа к информационным ресурсам корпоративной сети:

1) лица, имеющие доступ к информации, составляющую персонифицированную и служебную тайну;

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 секрет и служебную тайну, но задействованные в технологии обработки, передачи и хранения информации;

4) обслуживающий персонал.

14. Для построения моделей потенциальных нарушителей необходимо принять во внимание виды наиболее возможных нарушений и интересы различных лиц и организаций, а также имеющиеся в Обществе интересы других юридических лиц.

15. В Обществе возможны следующие виды нарушений:
1) несанкционированное использование программ, способных негативно повлиять на работоспособность КСПД Общества, снизить ее производительность, а также мешающих корректной работе КСПД (сканеры сети, интенсивный широковещательный трафик и т.п.);
2) использование прав локальных администраторов на рабочих станциях пользователей, что дает возможность установки обычному пользователю неограниченного количества программ;
3) использование прав администраторов на серверах, коммуникационном и прочем оборудовании с целью вредоносного изменения конфигурационных файлов, подмены, копирования и удаления файлов систем, журналов и конфигураций;
4) нарушения сотрудниками вследствие незнания требований информационной безопасности и нормативных правовых актов Общества.

16. Потенциальные внешние нарушители:
1) бывшие сотрудники и вспомогательный персонал;
2) посетители (приглашенные представители организаций, граждане);
3) представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.

7. СРЕДСТВА И МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

17. Средства и меры защиты от утечки информации по каналам связи:
1) Защита информации от утечки по каналам их передачи из/в Общества достигается путем применения комплексных программных, технических средств защиты и организационных мер.
2) Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их опасности в пределах контролируемой зоны. Закрытие и локализация каналов утечки обеспечивается организационно-техническими мерами.
3) В соответствии с используемыми каналами передачи электронной информации в Обществе предусматриваются необходимые технические средства защиты (межсетевой экран на основе Microsoft Forefront Threat Management Gateway, антивирусное ПО Kaspersky Endpoint Security, средства резервного копирования Акронис Инфозащита и Effector Saver).

18. Меры по защите от несанкционированного доступа к ресурсам сети NKZU.Net:
1) регистрация сотрудников и профессорско-преподавательского состава в сети производится администратором домена согласно ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

2) регистрация обучающихся в сети производится согласно ВНД СКГУ 12 Правила работы в компьютерных классах.

3) доступ к базе данных пользователей имеет администратор домена. Пароли пользователей хранятся в БД в зашифрованном виде.

4) при регистрации в сети NKZU пользователь получает доступ к корпоративной почте.

5) правила пользования корпоративной почтой регламентируются ВНД СКГУ 97 Положение о корпоративной электронной почте СКГУ им. М.Козыбаева.

19. Меры по защите СВТ:

1) Защита СВТ от НСД в Обществе строится по нескольким направлениям. Создаются автоматизированные средства регистрации пользователей, система блокирования учетных записей в соответствии с ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

2) Определяются организационные меры по предотвращению НСД, в том числе в случае утраты/компрометации паролей и выхода из строя СВТ согласно ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

3) В случае обнаружения фактов НСД к информационным ресурсам и системам Общества или выявления потенциальной угрозы информационной безопасности сотрудники ДИО немедленно информируют директора ДИО.

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

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

2) Для защиты от нелегального внедрения и использования неучтенных программ в Обществе кроме мероприятий, включающих физическую защиту, проведение аудита обращения к СВТ и мониторинг системных журналов, устанавливается базовый комплекс программного обеспечения, который необходимо устанавливать на рабочие станции пользователей. В базовый комплекс включается лицензионное программное обеспечение, необходимое для обеспечения работоспособности СВТ.

3) Использование для производственных целей прикладного ПО, внешних носителей информации, не входящего в состав базового комплекса, санкционируется отделом технического сопровождения по согласованию с руководителем ОТС.

21. Защита от действий вредоносных программ, вирусов:

1) В целях защиты от действий вредоносных программ и вирусов в Обществе используются антивирусные программные средства, защищенные от возможности несанкционированной модификации.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

2) Обновление баз антивирусного ПО происходит автоматически согласно расписанию сервера администрирования антивирусного ПО.

22. Защита информации в СВТ:

1) За каждым СВТ закрепляется сотрудник Общества. На СВТ используется система авторизации и/или аутентификации сотрудника, работающего на нем. Передача СВТ в пользование другому сотруднику, осуществляется по требованию с разрешения руководителя подразделения.

2) Правила пользования СВТ регламентированы в ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

23. Защита информации на официальном сайте Общества:

1) Доступ к размещению информации на официальном сайте общества предоставляется сотрудникам Общества в соответствии с ПП СКГУ 09 Положение о веб-сайте Северо-Казахстанского государственного университета.

2) Защита передаваемой информации обеспечивается использованием протокола HTTPS, который шифрует передаваемые сайтом данные.

3) Сервер сайта базируется на операционной системе семейства Linux.

24. Защита от ошибок программно-аппаратных средств:

1) С целью проверки работоспособности, перед вводом в эксплуатацию программные продукты и аппаратные средства подлежат тестированию в условиях максимально приближенных к реальным. Не пригодные к использованию программное обеспечение и аппаратные средства в эксплуатацию не принимаются.

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

1) Средства защиты КСПД вводятся в эксплуатацию, сопровождаются и используются в соответствии с установленным регламентом. Контроль за этим процессом осуществляют инженера ОТС, обеспечивающий информационную безопасность.

2) Сопровождением серверов Общества занимается инженера ОТС и инженера отдела программирования и информационного контента (далее - ОПИК).

26. Защита СВТ от нарушений работоспособности или разрушения аппаратных, программных, информационных ресурсов:

1) В результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций могут возникнуть нарушения работоспособности СВТ, а также разрушение аппаратных, программных, информационных ресурсов в Обществе. На такие случаи предусматриваются соответствующие меры защиты в соответствии с ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

27. Защита от незаконного подключения к корпоративной сети передачи данных:

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

1) 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.

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

1) Повреждение, некорректное функционирование, частичный, полный отказ сетевого оборудования Общества может быть, в первую очередь, в результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций.

2) 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.

29. Защита от неправомерного включения, выключения оборудования:

1) 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 руководителем ОТС.

30. Меры по защите системы архивирования:

1) Определяется порядок резервного копирования, хранения и восстановления программных продуктов и информационных систем. Хранилище резервных копий размещается в специально оборудованном помещении. Обеспечивается санкционированный доступ к хранилищу резервных копий для своевременного восстановления информации и информационных систем в случае сбоя, аварии и иных нештатных ситуациях.

2) Резервное копирование серверов и сетевых дисков подразделений Общества осуществляется в автоматическом режиме программным обеспечением Акронис Инфозащита на специально выделенный сервер не реже одного раза в месяц.

8. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

31. Директором ДИО инициируется проведение аудита информационной безопасности.

32. Аудит информационной безопасности проводится:

1) внутренним аудитором раз в полгода.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

2) независимыми экспертами (внешними организациями), обладающими специальными знаниями и опытом работы в сфере информационно-коммуникационных технологий один раз в год.

33. Результаты аудита информационной безопасности служат основанием для пересмотра настоящего Положения и внесения в него необходимых корректировок.

9. ПЕРЕСМОТР ПОЛОЖЕНИЯ

34. Пересмотр настоящего Положения проводится в случае:
1) внесения существенных изменений в ИС Общества,
2) изменений в законодательстве, организационной структуре Общества,
3) возникновения инцидентов информационной безопасности.

35. 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 информационных систем;
4) отчеты об инцидентах в области информационной безопасности

36. Пересмотр Положения об информационной безопасности должен осуществляться в соответствии с руководством по реализации Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 17799-2006/2009.

37. Настоящее Положение подлежит обязательному пересмотру по результатам проведения анализа и оценки рисков информационной безопасности Общества.

10. ОТВЕТСТВЕННОСТЬ

38. Все пользователи СВТ обязаны использовать компьютерные ресурсы квалифицированно, эффективно, придерживаясь правил этики.

39. Правила пользования СВТ, КСПД и ИС регламентированы ПП СКГУ 08 Положение о компьютерной сети NKZU.net. За нарушение правил пользования СВТ, КСПД и ИС пользователь привлекается к дисциплинарной ответственности согласно ВНД СКГУ 87 Правила наложения дисциплинарных взысканий на работников на СКГУ им. М. Козыбаева.

40. Сотрудники Общества за нарушение требований пунктов настоящего Положения будут привлекаться к административной или иной ответственности, в соответствии с действующим законодательством Республики Казахстан.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

41. Администраторы ресурсов ИС обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для обеспечения информационной безопасности.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

42. Утверждение Положения, а также внесение изменений и дополнений в него относится к компетенции Совета директоров Общества.
43. 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 до момента внесения соответствующих изменений в настоящее Положение.

Рассмотрено на заседании Правления
Протокол № 12 от 29.03.2021 г.

РАЗРАБОТАНО:

Директор ДИО — Д. Мораш

СОГЛАСОВАНО:

И.о. заместителя Председателя Правления-Ректора — Е. Исакаев

Главный комплаенс академ офицер — И. Джемалединова

Главный менеджер по цифровизации — И. Курмашев

Инженер отдела технического сопровождения — А. Брындин

Сотрудник ДКНБ по СКО — Р. Гиматдинов

Заместитель директора по информационным технологиям НУО «Гуманитарно-технический колледж» — А. Бодряков

Директор ТОО «Межрегиональный Центр новых технологий» — А. Чернышов

Корпоративтік хатшының қолы
Подпись корпоративного секретаря: