УТВЕРЖДЕНО
Решением Совета директоров
НАО «Кокшетауский университет
имени Ш.Уалиханова»
(протокол № 10 от 14.06.2021 г.)

ПОЛОЖЕНИЕ
об информационной безопасности
НАО «Кокшетауский университет имени Ш.Уалиханова»

1.ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение об информационной безопасности (далее - Положение) учитывает современное состояние и ближайшие перспективы развития корпоративной сети передачи данных (далее – КСПД) НАО «Кокшетауский университет имени Ш.Уалиханова» (далее – Общество), цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее ресурсов.

2. Требования Положения распространяются на структурные подразделения Общества, подведомственные им организации, 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: отдел компьютерных технологий и телекоммуникаций и юридический отдел.

4. Сотрудники отдела компьютерных технологий и телекоммуникаций, руководитель юридического отдела, руководитель департамента финансов, руководитель отдела кадров проводят необходимые технические и организационные мероприятия для обеспечения информационной безопасности.

5. Проректор по интернационализации и развитию инфраструктуры осуществляет мероприятия по защите корпоративных секретов, обеспечению

информационной безопасности и режима секретности в Обществе и подведомственных организациях.

6. Руководитель отдела компьютерных технологий и телекоммуникаций (далее - ОКТТ) осуществляет организацию квалифицированной разработки (совершенствования) системы защиты информации и организационного (административного) обеспечения ее функционирования в Обществе.

2. ЦЕЛИ И ЗАДАЧИ

7. 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.

8. Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния корпоративной сети передачи данных:

- доступность обрабатываемой информации для зарегистрированных пользователей;
- устойчивое функционирование КСПД Общества;
- обеспечения конфиденциальности информации, хранимой, обрабатываемой средствами вычислительной техники (далее - СВТ) и передаваемой по каналам связи;
- целостность и аутентичность информации, хранимой и обрабатываемой информационной системой (далее - ИС) Общества и передаваемой по каналам связи.

9. Для достижения поставленной цели необходимо решить следующие задачи:

- защита от вмешательства посторонних лиц в процесс функционирования информационных ресурсов Общества;
- разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и криптографическими средствами защиты, используемыми в ИС;
- регистрация в системных журналах действий пользователей при использовании сетевых ресурсов;
- периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов специалистами информационной безопасности;
- контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
- защита информации от несанкционированной модификации, искажения;
- контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносного программного обеспечения;
- защиту служебной тайны и персональных данных от утечки,

несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;

- обеспечение авторизации и аутентификации пользователей, участвующих в информационном обмене;
- своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;
- создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
- 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.
- создание и обеспечения бесперебойной работы электронного документооборота.
- постоянный аудит политики безопасности внутренним аудитом не реже 1 раза в полгода и внешним аудитом раз в год.

3. ПОЛЬЗОВАТЕЛИ ИНФОРМАЦИОННЫХ СИСТЕМ

10. К пользователям информационных систем относятся:

- сотрудники – служащие, осуществляющие свою деятельность в Обществе и обладающие основными правами и обязанностями в соответствии с законодательством Республики Казахстан;
- вспомогательный персонал – обслуживающий и технический персонал подведомственных и 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-системотехники, технические специалисты;
- специалисты по информационной безопасности (специальных средств защиты) и др.;
- потребители услуг – лица и/или сторонние организации, использующие информационные ресурсы Общества;
- студенты, интерны, резиденты, магистранты и докторанты.

4. МОДЕЛИ ПОТЕНЦИАЛЬНЫХ НАРУШИТЕЛЕЙ

11. 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.

12. Потенциальных нарушителей можно разделить на внутренних и внешних. Внутренними нарушителями могут быть практически все сотрудники Общества и вспомогательный персонал. Их можно разделить на следующие группы в зависимости от уровня доступа к информационным ресурсам корпоративной сети:

- лица, имеющие доступ к информации, составляющую персонифицированные и служебную тайну;
- лица, имеющие доступ к информации, составляющую служебную тайну и задействованные в технологии обработки, передачи и хранения информации;
- лица, не имеющие доступ к информации, составляющую персонифицированные секрет и служебную тайну, но задействованные в технологии обработки, передачи и хранения информации;
- обслуживающий персонал.

13. Чтобы построить реальную модель потенциального нарушителя необходимо принять во внимание виды выявленных нарушений, устремлений различных лиц и организаций, а также имеющиеся в Обществе интересы других юридических лиц.

14. В Обществе возможны следующие виды нарушений:

- несанкционированное использование программ, могущих негативно повлиять на работоспособность КСПД Общества, снизить ее производительность, а также мешающих корректной работе КСПД (сканеры сети, интенсивный широковещательный трафик и т.п.);
- использование прав локальных администраторов на рабочих станциях пользователей, что дает возможность установки обычному пользователю неограниченного количества программ;
- нарушения сотрудниками вследствие незнания требований информационной безопасности и нормативных правовых актов Общества.

15. Потенциальные внешние нарушители:

- бывшие сотрудники и вспомогательный персонал;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности (энерго-, водо-, теплоснабжения и т.п.);
- посетители (приглашенные представители организаций, граждане);
- представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.

5. НАЗНАЧЕНИЕ, НОРМАТИВНАЯ И ПРАВОВАЯ БАЗА ПОЛОЖЕНИЯ

16. Настоящее Положение детализирует требования по решению вопроса обеспечения информационной безопасности в единой информационной

телекоммуникационной среде, объединяющей ИС Общества.

17. Положение информационной безопасности Общества является методологической базой:

- выработки и совершенствования комплекса согласованных нормативных, правовых, технологических и организационных мер, направленных на защиту информации;
- обеспечения информационной безопасности;
- координации деятельности территориальных и структурных подразделений при проведении работ по соблюдению требований обеспечения информационной безопасности.

18. Научно-методической основой Положения является системный подход, предполагающий проведение исследований, разработку системы защиты информации в процессе ее обработки в информационных системах с учетом всех факторов, оказывающих на нее влияние и комплексно- го применения различных мер и средств защиты.

19. Основные требования Положения базируются на качественном осмыслении вопросов информационной безопасности, не концентрируя внимание на экономическом (количественном) анализе рисков и обосновании необходимых затрат на защиту информации.

20. Нормативной и правовой базой Положения являются: Указ Президента Республики Казахстан от 14 ноября 2011 года № 174 «О Концепции информационной безопасности Республики Казахстан до 2016 года», Законы Республики Казахстан «О национальной безопасности Республики Казахстан», «О государственных секретах», «О противодействии терроризму», «Об электронном документе и электронной цифровой подписи», «Об информатизации», «О техническом регулировании», «О лицензировании», «О средствах массовой информации», «О связи» и иные акты Республики Казахстан и Общества, регламентирующие вопросы обеспечения информационной безопасности.

6. СРЕДСТВА И МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

6.1 Средства и меры защиты от утечки информации по каналам связи

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

22. 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.

23. В соответствии с используемыми каналами передачи электронной информации в Обществе предусматриваются необходимые технические средства защиты (межсетевой экран и т.п.). Организуется система

регистрации, передачи, приема и хранения носителей информации, предусматриваются надлежащие 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 Обществ для предотвращения доступа посторонних лиц.

6.2 Меры по защите средств вычислительной техники

24. Защита СВТ от несанкционированного доступа в Обществе строится по нескольким направлениям. Создаются автоматизированные средства регистрации пользователей, система блокирования учетных записей и оповещения сотрудников об угрозе или проникновении в СВТ.

25. Определяются организационные меры по предотвращению несанкционированного доступа (далее - НСД), в том числе в случае утраты/компрометации паролей и выхода из строя СВТ.

26. В случае обнаружения фактов НСД к информационным ресурсам и системам Общества или выявления потенциальной угрозы информационной безопасности сотрудники ОКТТ немедленно информирует руководителя, курирующего вопросы связи.

6.3 Защита от аппаратных спецвложений, нелегального внедрения и использования неучтенных программ

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

28. 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 (далее - ПО), необходимое для обеспечения работоспособности СВТ.

29. Использование для производственных целей прикладного ПО, внешних носителей информации не входящего в состав базового комплекса санкционируется ОКТТ по согласованию с руководителем, курирующим вопросы связи, информатизации и телекоммуникаций.

6.4 Защита от несанкционированного копирования данных пользователем

30. Служебная и иная защищаемая информация, обрабатываемая и хранящаяся в информационных системах Общества, подлежит копированию

и передаче третьему лицу только с разрешения ректора по согласованию с руководителем, курирующим вопросы связи, информатизации и телекоммуникаций.

31. За копирование и передачу служебной и иной защищаемой информации третьему лицу без разрешения, пользователь привлекается к дисциплинарной ответственности.

6.5 Защита информации, отображаемой на мониторе средств вычислительной техники

32. Защита достигается путем ограничения физического доступа к средствам отображения информации, исключения наблюдения за отображаемой информацией посторонними лицами.

6.6 Защита от действий вредоносных программ, вирусов

33. В целях защиты от действий вредоносных программ и вирусов в Обществе используются «иммуностойкие» программные средства, защищенные от возможности несанкционированной модификации, специальные программы-анализаторы, осуществляющие постоянный контроль за возникновением отклонений в деятельности прикладных программных продуктов, периодическую проверку наличия возможных следов вирусной активности, а также входной контроль новых программ перед их использованием.

6.7 Защита от хищения носителей информации

34. В Обществе устанавливается определенный порядок хранения и использования носителей информации.

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

6.8 Защита информации в средствах вычислительной техники

36. 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 с разрешения руководителя подразделения. Принимаются необходимые программно-технические средства защиты информации, обрабатываемой на СВТ.

6.9 Защита от умышленной модификации информации

37. Кроме средств регламентированного доступа к СВТ защита информации от модификации осуществляется программными, техническими и организационными мерами. Для своевременного выявления и обнаружения указанных посягательств используются журналы действий операторов и администраторов.

6.10 Защита от ошибок программно-аппаратных средств

38. 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.

6.11 Защита от некомпетентного использования, настройки или неправомерного отключения средств защиты

39. Средства защиты КСПД вводятся в эксплуатацию, сопровождаются и используются в соответствии с установленным регламентом. Контроль за этим процессом осуществляет ОКТТ, обеспечивающий информационную безопасность.

40. Сопровождением серверов Общества занимается ОКТТ.

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

6.12 Защита средств вычислительной техники от нарушений работоспособности или разрушения аппаратных, программных, информационных ресурсов

42. 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, согласно Плану по обеспечению непрерывной деятельности информационных систем Общества.

6.13 Защита от ввода ошибочных данных

43. Данные, вводимые в приложениях, проверяются программными и техническими средствами, чтобы гарантировать их правильность и соответствующее использование. Ввод информации осуществляется уполномоченным на это персоналом.

6.14 Меры по защите коммуникационных средств

44. Основные и резервные телекоммуникационные сервисы соответствующим образом отделяются друг от друга, чтобы не подвергаться одним и тем же угрозам.

6.15 Защита от незаконного подключения к корпоративной сети передачи данных

45. 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 попытка незаконного подключения к линиям связи и сетевому оборудованию лица несут ответственность в соответствии с законодательством Республики Казахстан.

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

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

47. 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.

48. Разрабатывается План обеспечения непрерывной работы и восстановления, согласно Плану по обеспечению непрерывной деятельности информационных систем Общества.

6.17 Защита от неправомерного включения, выключения оборудования

49. 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 ОКТТ и руководителем, курирующим вопросы связи, информатизации и телекоммуникации.

6.18 Защита от неправомерной модификации передаваемых данных, технической и служебной информации

50. Кроме средств санкционированного доступа к коммуникационным средствам и сетевому оборудованию, защита передаваемых данных от модификации осуществляется программно-техническими и организационными мерами.

6.19 Меры по защите системы архивирования

51. Определяется порядок резервного копирования, хранения и восстановления программных продуктов и информационных систем. Хранилище резервных копий размещается в помещении специально оборудованным согласно Плану по обеспечению непрерывной деятельности информационных систем. Обеспечивается санкционированный доступ к хранилищу резервных копий для своевременного восстановления информации и информационных систем в случае сбоя, аварии и иных нештатных ситуациях.

32. Разрабатывается План по обеспечению непрерывной деятельности информационных систем, в котором также определяются меры по защите

архивов на случай возникновения аварий, стихийных бедствий и других нештатных ситуаций.

6.20 Прочие меры по защите информации

33. Следует принять исчерпывающие меры защиты информации на всех запоминающихся устройствах при передаче СВТ на ремонт сторонним организациям.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

34. Соблюдение требований Положения информационной безопасности обязательно для всех пользователей информационных систем Общества. Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации. Результаты аудита могут служить основанием для пересмотра некоторых пунктов Положения и внесения в них необходимых корректировок. Аудит информационной безопасности Общества целесообразно проводить ежегодно, по итогам которого ОКТТ должен проводиться пересмотр Положения на предмет соответствия предъявляемым требованиям, в случае возникновения необходимости вносить изменения и дополнения.