УТВЕРЖДАЮ
Ректор Учреждения «SDU University»
_____ Игенбаев А. Б.
«__11__» ___февраля___ 2025 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УЧРЕЖДЕНИЯ «SDU UNIVERSITY»

Каскелен, 2025 г.

СОДЕРЖАНИЕ

1. Введение 4

2. Сокращения, термины и определения, используемые в данном документе 4

3. Пользователи информационных систем 6

4. Модель нарушителя 6

4.1 Потенциальные нарушители 6

5. Политика информационной безопасности 8

5.1. Назначение, нормативная и правовая база Политики 8

5.2. Цели и задачи Политики информационной безопасности 9

5.2.1 Цели Политики 9

5.2.2 Задачи Политики 9

5.3. Меры по реализации Политики 10

5.3.1. Меры по защите от утечки по каналам их передачи 10

5.3.1.1 Средства и меры защиты от утечки по техническим каналам 10

5.3.2. Меры по защите СВТ 11

5.3.2.1 Защита от НСД к СВТ 11

5.3.2.2 Защита от использования незарегистрированных носителей информации 11

5.3 Защита от аппаратных спецвложений, нелегального внедрения и использования неучтенных программ 11

5.4 Защита от несанкционированного копирования данных пользователем. 11

5.5 Защита информации, отображаемой на мониторе СВТ 12

5.6 Защита от действий вредоносных программ, вирусов 12

5.7 Защита от хищения носителей информации 12

5.8 Защита информации в оперативной памяти 12

5.9 Защита от умышленной модификации информации 12

5.10 Защита от ошибок программно-аппаратных средств 13

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

5.12 Защита от частичного или полного отказа СВТ или разрушению аппаратных, программных, информационных ресурсов. 13

5.13 Защита от ввода ошибочных данных 13

5.14 Защита от атак типа «отказ в обслуживании» со стороны сети 13

5.15 Меры по защите коммуникационных средств 14

5.16 Защита от незаконного подключения к линиям связи и к сетевому оборудованию 14

5.17 Защита от повреждения, некорректного функционирования, частичного или полного отказа сетевого оборудования 14

5.18 Защита от неправомерного включения, выключения оборудования 14

5.19 Защита от неправомерной модификации передаваемых данных, технической и служебной информации 15

5.20 Меры по защите системы архивирования 15

5.21 Меры по защите при выводе информации 15

5.22 Пересмотр политики информационной безопасности 15
6. Перечень законодательных и нормативных правовых актов Республики Казахстан и иных документов 16

1. Введение

Политика информационной безопасности (далее-Политика) Учреждения «SDU University» (далее- Университета) — комплекс превентивных мер по защите информации, в том числе конфиденциальных данных, информационных процессов и включает в себя требования в адрес персонала, менеджеров и технических служб. На основе Политики строится управление информационной безопасностью.

Настоящая Политика учитывает современное состояние и ближайшие перспективы развития локальной вычислительной сети Университета, цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее ресурсов.

Положения и требования Политики распространяются на их структурные подразделения Университета, в которых осуществляется автоматизированная обработка информации, в том числе конфиденциальных сведений или персональных данных, а также субъектов, осуществляющих сопровождение, обслуживание и обеспечение функционирования Университета. Основные положения Политики распространяются на другие организации и учреждения, осуществляющие взаимодействие с Университетом в качестве поставщиков и потребителей (пользователей) информации.

2. Сокращения, термины и определения, используемые в данном документе

Основные термины и определения, используемые в Политике, приведены согласно стандартам СТ РК 34.015-2002 **«Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы»**, СТ РК ISO/IEC 27001-2023 **«Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасностью. Требования»**, СТ РК ISO/IEC 27002-2023 **«Информационная безопасность, кибербезопасность и защита конфиденциальности. Средства управления информационной безопасностью»**.

При разработке данного документа использовались следующие понятия:

Активы информационной системы - информационные, технические, программные и другие ресурсы, входящие в состав информационной системы;

Информационная безопасность — состояние защищенности ~~государетвенных~~ информационных ресурсов, а также прав личности и интересов общества в информационной сфере;

Информационная система - совокупность информационных технологий, информационных сетей и средств их программно-технического обеспечения, предназначенных для реализации информационных процессов;

Информационные ресурсы - электронная систематизированная информация (информационные базы данных), содержащаяся в информационных системах, объединенная соответствующим программным обеспечением и представляющая интерес для пользователей информации;

Информационные процессы – процессы, в том числе и технологические процессы создания, сбора, обработки, накопления, хранения, поиска, передачи, использования и распространения информации с использованием информационных технологий;

Информационные услуги - деятельность по предоставлению информационных ресурсов, информационных систем пользователям по их запросам или по соглашению сторон;

Информация с ограниченным доступом - информация, для которой установлен специальный режим распространения, сбора, обработки и использования;

Корпоративная вычислительная сеть - совокупность информационных систем, компьютеров, кабелей, сетевых адаптеров, объединённых в единую сеть и эксплуатируемых в Парламенте;

Конфиденциальная информация – информация, не составляющая государственные секреты, но содержащая сведения, доступ к которым ограничен в соответствии с законодательством Республики Казахстан.

Несанкционированный доступ (НСД) - доступ субъекта к объекту в нарушение установленных в системе правил разграничения доступа;

Объект - пассивный компонент системы, единица ресурса автоматизированной системы (устройство, диск, каталог, файл и т.п.), доступ к которому регламентируется правилами разграничения доступа;

Объект защиты - информация или носитель информации или информационный процесс, в отношении которых необходимо обеспечивать защиту в соответствии с поставленной целью защиты информации;

Правила разграничения доступа - совокупность правил, регламентирующих права доступа субъектов к объектам в некоторой системе;

Средства вычислительной техники – технические или программные средства, используемые для обработки, хранения и передачи информации, к которым относятся персональные компьютеры, серверное оборудование, активное сетевое оборудование, а также их периферийное оборудование и программное обеспечение.

Субъект - активный компонент системы (пользователь), действия которого регламентируются правилами разграничения доступа.

Специалист информационной безопасности (СИБ) – должностное лицо, ответственное за обеспечение защиты информационных ресурсов Университета. Функции СИБ исполняет Директор Центра Цифровизации либо иное лицо, уполномоченное приказом ректора.

Сокращения:

ИС	информационные системы
ЗИ	защита информации
ЛВС	локальная вычислительная сеть
НСД	несанкционированный доступ
ОС	операционная система
ОИТП	Отдел информационно-технической поддержки
СВТ	средства вычислительной техники
ПО	программное обеспечение
ПК	персональный компьютер

3. Пользователи информационных систем

К пользователям информационных систем относятся:

1) работники Университета:

- преподаватели;
- сотрудники производственных подразделений, в том числе разработчики, программисты и технический персонал сторонних организаций;

2) сотрудники непроизводственных подразделений;

- персонал, обеспечивающий информационную безопасность;
- вспомогательный персонал (охрана);

3) студенты Университета.

4. Модель нарушителя

4.1 Потенциальные нарушители

Потенциальных нарушителей можно разделить на внутренних и внешних.

Внутренними нарушителями могут быть практически все работники Университета. Их можно разделить на следующие группы в зависимости от уровня доступа к информационным ресурсам корпоративной сети:

- лица, имеющие доступ к информации, составляющую конфиденциальную и коммерческую тайну;

- лица, имеющие доступ к информации, составляющую коммерческую тайну и задействованные в технологии обработки, передачи и хранения информации;
- лица, не имеющие доступ к информации, составляющую конфиденциальную и коммерческую тайну, но задействованные в технологии обработки, передачи и хранения информации;

  обслуживающий персонал.

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

Выявлены следующие виды нарушений:

несанкционированное использование программ, могущих негативно повлиять на работоспособность ЛВС Университета, снизить её производительность, а также мешающих корректной ей ЛВС (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 работниками Университета вследствии незнания требований информационной безопасности и нормативных правовых актов Университета.

Потенциальные **внешние нарушители:**

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

Исходя из изложенного, можно выделить три основные модели потенциального нарушителя.

Модель № 1

Наиболее часто встречающий потенциальный нарушитель, это работники, действующие по незнанию требований информационной безопасности и нормативных правовых актов Университета, регламентирующих защиту информации. Их деяния не носят прямого умысла нанесения ущерба Университету, но могут привести к утечке, уничтожению, искажению информации, к частичному или полному выводу из строя информационных систем, локальной вычислительной сети.

Модель № 2

Потенциальный нарушитель, который действует целенаправленно, преследует цель получить доступ к конфиденциальной информации Университета.

Наиболее вероятно, что такие нарушители будут внедряться и вербоваться среди технического персонала, руководителей, ответственных работников (администраторы, разработчики ИС и персонал, сопровождающий программные продукты, программисты, тестировщики и внедренцы), а также сотрудников службы обеспечения информационной безопасности, которые по занимаемой должности имеют большой уровень доступа к информационным ресурсам.

Для получения информации потенциальный нарушитель может вступать в сговор с работниками Университета, может устанавливать программы для удаленного управления их ПК.

Модель № 3

Потенциальный нарушитель, так называемый хакер, которые для самоутверждения, подтверждения своих знаний и способностей в области информационных технологий совершает атаки на различные системы, и желает получить несанкционированный доступ к ЛВС Университета.

Лица и организации, желающие нанести ущерб Университету по различным мотивам.

5. Политика информационной безопасности

5.1. Назначение, нормативная и правовая база Политики

Политика информационной безопасности Университета 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.

Научно-методической основой Политики 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 комплексного применения различных мер и средств защиты.

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

Нормативной и правовой базой Политики являются Конституция Республики Казахстан, Гражданский и Уголовный кодексы, законы, указы, постановления и иные акты Республики

Казахстан и Университета, регламентирующие вопросы обеспечения информационной безопасности.

5.2. Цели и задачи Политики информационной безопасности

5.2.1 Цели Политики

Главной целью, на достижение которой направлены все положения Политики, является надежное обеспечение информационной безопасности и как следствие недопущение нанесения материального, физического, морального или иного ущерба Университету в результате информационной деятельности.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния корпоративной вычислительной сети:

- доступность обрабатываемой информации для зарегистрированных пользователей;
- устойчивое функционирование ЛВС Университета;
- обеспечения конфиденциальности информации, хранимой, обрабатываемой СВТ и передаваемой по каналам связи;
- целостность и аутентичность информации, хранимой и обрабатываемой в ЛВС Университета и передаваемой по каналам связи.
- основные бизнес-процессы: кадровые процедуры, финансовые процедуры и бухгалтерский учет, делопроизводство, академические процессы и другие сопутствующие процессы должны быть организованы в специализированных информационных системах, защищенных надлежащим образом в рамках данной политики и с контролем доступа.

5.2.2 Задачи Политики

Для достижения поставленных целей необходимо решить следующие задачи:

- защита от вмешательства посторонних лиц в процесс функционирования ЛВС Университета;
- разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и криптографическими средствами защиты, используемыми в ЛВС Университета;
- регистрация действий пользователей при использовании ресурсов ЛВС Университета в системных журналах;
- 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 вредоносных кодов, включая компьютерные вирусы;

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

● обеспечение 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 для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

5.3. Меры по реализации Политики

5.3.1. Меры по защите от утечки по каналам их передачи

5.3.1.1 Средства и меры защиты от утечки по техническим каналам

Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их энергетической опасности на границах контролируемой зоны (территории, помещения). Закрытие и локализация каналов утечки обеспечивается организационно-техническими мерами.

В соответствии с используемыми каналами передачи информации в Университете предусматриваются адекватные технические средства защиты. 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 Университета, организуется пропускной режим для предотвращения доступа посторонних лиц в Университет.

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

5.3.2. Меры по защите СВТ

5.3.2.1 Защита от НСД к СВТ

Защита СВТ пользователей от несанкционированного доступа в Университет, строится по нескольким направлениям. Создаются автоматизированные средства регистрации пользователей,

система блокирование учетных записей и оповещения работников об угрозе или проникновении в СВТ.

Определяются организационные меры по предотвращению НСД, в том числе в случае утраты/компрометации паролей и выхода из строя СВТ.

5.3.2.2 Защита от использования незарегистрированных носителей информации

Запись и копирование служебной и иной защищаемой информации, в том числе для передачи другим лицам, производится на зарегистрированные в установленном порядке носители информации. За запись служебной и иной защищаемой информации на незарегистрированные в установленном порядке носители, пользователь привлекается к дисциплинарной и иной, предусмотренной законодательством Республики Казахстан, ответственности.

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

Для защиты от аппаратных спецвложений, нелегального внедрения и использования неучтенных программ в Университете 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 ПО, необходимое для обеспечения работоспособности СВТ.

Использование для производственных целей прикладного ПО, не входящего в состав базового комплекса, санкционируется администратором информационной безопасности.

5.4 Защита от несанкционированного копирования данных пользователем.

За копирование и передачу служебной и иной защищаемой информации третьему лицу без разрешения руководства Университета, пользователь привлекается к дисциплинарной ответственности и иной предусмотренной законодательством РК.

5.5 Защита информации, отображаемой на мониторе СВТ

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

5.6 Защита от действий вредоносных программ, вирусов

В целях защиты от действий вредоносных программ и вирусов в Университете 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;

Организационные меры, включают в себя разработку нормативных правовых актов Университета, регламентирующие эту деятельность и проведение работ в соответствии с ними.

5.7 Защита от хищения носителей информации

В Университете устанавливается определенный порядок хранения и использования носителей информации, в том числе сведений в электронном виде. При передаче носителя цифровой информации для повторного использования за пределами Университета проводится его очистка с целью исключения несанкционированного разглашения защищаемых сведений.

5.8 Защита информации в оперативной памяти

За каждым СВТ закрепляется работник Университета. На СВТ используется система аутентификации и идентификации сотрудника, работающего на нем. Передача СВТ в пользование другому работнику осуществляется с разрешения руководителя подразделения. Принимаются необходимые программно-технические средства защиты информации, обрабатываемой на СВТ.

5.9 Защита от умышленной модификации информации

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.

5.10 Защита от ошибок программно-аппаратных средств

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

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

Средства защиты локальной вычислительной сети вводятся в эксплуатацию, сопровождаются и используются в соответствии с установленным регламентом. Контроль за этим процессом осуществляет подразделение Университета, обеспечивающее информационную безопасность.

Сопровождением серверов Университета занимается персонал отдела АИВС Университета. Все действия персонала по сопровождению регламентированы. При нарушении регламента причастные сотрудники привлекаются к ответственности

5.12 Защита от частичного или полного отказа СВТ или разрушению аппаратных, программных, информационных ресурсов.

Частичный, полный отказ СВТ, а также разрушение аппаратных, программных, информационных ресурсов в Университете может возникнуть в результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций. На такие случаи в Университете предусматриваются соответствующие меры защиты и План обеспечения непрерывной работы и восстановления.

5.13 Защита от ввода ошибочных данных

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

5.14 Защита от атак типа «отказ в обслуживании» со стороны сети

В целях защиты от атак типа «отказ в обслуживании» враждебного мобильного кода проводятся организационные и технические мероприятия, включающие в себя разработку нормативных правовых актов Университета, регламентирующие эту деятельность и проведение работ в соответствии с ними.

5.15 Меры по защите коммуникационных средств

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

5.16 Защита от незаконного подключения к линиям связи и к сетевому оборудованию

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 действующим законодательством.

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

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

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

Разрабатывается План обеспечения непрерывной работы и восстановления.

5.18 Защита от неправомерного включения, выключения оборудования

Сетевое оборудование локальной вычислительной сети Университета вводится в эксплуатацию, сопровождается и используется в соответствии с установленным регламентом. Включение и отключение оборудования производится уполномоченным техническим персоналом, который работает в соответствии с указанием руководства Университета.

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

Кроме средств санкционированного доступа к коммуникационным средствам и сетевому оборудованию, защита передаваемых данных от модификации осуществляется программно-техническими и организационными мерами. Для своевременного выявления, предупреждения и пресечения указанных посягательств используется аппаратура наблюдения и мониторинга.

5.20 Меры по защите системы архивирования

Определяется порядок резервного копирования, хранения и восстановления программных продуктов и информационных систем, Хранилище резервных копий размещается в помещении за пределами основного здания Университета на расстоянии не менее 2-3 километров. Обеспечивается санкционированный доступ к хранилищу резервных копий для своевременного восстановления информации и информационных систем в случае сбоя, аварии и иных нештатных ситуациях.

Разрабатывается План обеспечения непрерывной работы и восстановления, в котором также определяются меры по защите архивов на случай возникновения аварий, стихийных бедствий и других нештатных ситуаций.

5.21 Меры по защите при выводе информации

Основными устройствами вывода информации являются мониторы, принтеры, средства записи информации на цифровые носители. Основные меры по защите информации уже приведены выше.

Следует принять исчерпывающие меры защиты информации на устройствах долговременной памяти при передаче СВТ на ремонт и сторонние организации.

5.22 Пересмотр политики информационной безопасности

Соблюдение требований Политики информационной безопасности обязательно для всех работников Университета. Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации. Результаты аудита могут служить основанием для пересмотра некоторых положений Политики и внесения в них необходимых корректировок.

Ежегодно целесообразно проводить аудит информационной безопасности Университета, Центром Цифровизации должен производиться пересмотр Политики ИБ на предмет соответствия предъявляемым требованиям. В случае возникновения необходимости, при выявлении в процессе аудита несоответствия современным требованиям, вносить изменения и дополнения.

Кроме этого, используемые информационные технологии и организация служебной деятельности непрерывно меняются, это приводит к необходимости корректировать существующие подходы к обеспечению информационной безопасности.

6. Перечень законодательных и нормативных правовых актов Республики Казахстан и иных документов

1. Закон Республики Казахстан от 24 ноября 2015 года № 217-III «Об информатизации»
2. Закон Республики Казахстан от 05.07.2004 г. «О связи»
3. Указ Президента «О Концепции информационной безопасности РК до 2016 года» от 14 ноября 2011 года № 174.
4. Постановление Правительства Республики Казахстан от 28 марта 2023 года № 269 «Об утверждении Концепции цифровой трансформации, развития отрасли информационно-коммуникационных технологий и кибербезопасности на 2023 — 2029 годы».
5. Постановление Правительства Республики Казахстан от 20.12.2016 г. № 832 «Об утверждении единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности»

Лист ознакомления

№	ФИО	Должность	Дата	Подпись