МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН

МЕЖДУНАРОДНЫЙ ТАРАЗСКИЙ ИННОВАЦИОННЫЙ ИНСТИТУТ

УТВЕРЖДАЮ
Ректор Международного Таразского инновационного института, д.ф.н., профессор
_____Е.Б. Саурыков
«24» _____2021 г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Тараз 2021

ПРЕДИСЛОВИЕ

1.РАЗРАБОТАНО И ВНЕДРЕНО	**Управление информационно-коммуникационных технологий**
2. РАЗРАБОТЧИКИ	**Первый проректор, д.и.н. А.Б. Абдуалы**
	Начальник управления по академической политике Д.К. Акимова
	Начальник управления ИКТ Т.Н.Тулеев

3. РАССМОТРЕНО И УТВЕРЖДЕНО НА УЧЕНОМ СОВЕТЕ ИНСТИТУТА
№ 11 от «24» 06 2021 г.

Содержание

1. Область применения

1. Политика информационной безопасности разработана в соответствии с Конституцией РК от 30 августа 1995 года (с изменениями и дополнениями по состоянию от 23 марта 2019 года) и Законом РК «Об информатизации» от 24 ноября 2015 года.

2. В настоящее время сформировалось устойчивое отношение к информации всех видов, как к ценнейшему ресурсу. Объясняется это небывалым ростом объема информационных потоков в современном обществе. В первую очередь это относится к тем направлением государственной деятельности, которые являются наиболее важными в жизнеобеспечении общества, а именно: экономика: наука; образование: социальная сфера; др. Все эти направления тесно пересекаются, и развитие каждого напрямую зависит от качества используемой информации, ее достоверности и полноты, оперативности и формы представления. Для обеспечения надежной защиты, необходимо постоянно держать во внимании, и анализировать всевозможные источники угроз, сопоставлять по уязвимости и определять потенциальные угрозы, реализация которых прямо или косвенно может нанести вред информационной системе (далее - ИС) Международного инновационного института (МТИИ).

3. Учитывая тенденции развития мировой и отечественной экономики, в соответствии с которыми, информация и информационные технологии становятся важнейшими активами современного образования, способствующими повышению его конкурентоспособности. МТИИ уделяет особое внимание решению задачи обеспечения информационной безопасности (далее - ИБ).

4. Под ИБ, институт понимает состояние защищенности своих интересов (целей) от угроз в информационной сфере. Защищенность достигается обеспечением совокупности свойств информационных активов: конфиденциальности, целостности и доступности. Обеспечение ИБ института осуществляется в рамках циклической модели менеджмента ИБ «планирование — реализация — проверка совершенствование», отвечающей принципам и модели корпоративного менеджмента в МТИИ.

5. Политика информационной безопасности представляет собой совокупность требований, правил, положений и принятых решений, определяющих:

порядок доступа к информационным ресурсам;

необходимый уровень (класс и категорию) защищенности объектов информатизации; организацию защиты информации в целом: дополнительные требования по защите отдельных компонентов: основные направления и способы защиты информации.

2. Введение

2.1. Требования, установленные в Политике информационной безопасности (далее - Политика ИБ), носят общий характер и предназначены для применения ко всем структурным подразделениям, распространяются на всех работников института, имеющих доступ к информационным активам и ИТ - инфраструктуре.

3. Общие положения

3.1. Настоящая Политика ИБ МТИИ устанавливает цели, задачи и принципы в области ИБ, которыми руководствуется институт в своей деятельности, определяет требования для создания, внедрения, эксплуатации, постоянного контроля, анализа, поддержания в рабочем состоянии и улучшения документированной система менеджмента защиты информации, также определяет требования для реализации средств управления информационной безопасностью, приспособленных к потребностям института и отдельных структурных подразделений института.

3.2. Политика ИБ МТИИ определяет и описывает решение об осуществлении целенаправленной систематической деятельности по обеспечению ИБ; общий подход к распределению ответственности за обеспечение ИБ внутри института; указание на необходимость для всего персонала соблюдать определенные меры предосторожности при работе с информацией и ИС, повышать свою квалификацию в данной области и осознавать меру ответственности за возможные нарушения; отношение руководства МТИИ к фактам нарушения требований по обеспечению ИБ и лицам, совершающим такие нарушения, а также общий подход к их преследованию в случае выявления таких фактов.

3.3. Политика ИБ служит для формулирования и демонстрации отношения руководства МТИИ к вопросам ИБ и отражения общих целей всего института в этой области; основой для разработки индивидуальных политик безопасности (на более низких уровнях), правил и инструкций, регулирующих отдельные вопросы: средством информирования работников об основных задачах и приоритетах института в сфере ИБ.

3.4. Политика ИБ определяет отношение института (руководства) к определенным аспектам его деятельности и функционирования информационных систем: отношение и требования к отдельным информационным потокам и ИС, обслуживающим различные сферы деятельности, степень конфиденциальности, доступности, целостности информации, а также требования к надежности (например, в отношении финансовой информации, а также ИС и персонала, которые относятся к ней); отношение и требования к определенным информационным и телекоммуникационным технологиям, методам и подходам к обработке информации и построения ИС; отношение и требования к сотрудникам Института как к участникам процессов обработки информации, от которых напрямую зависит эффективность многих процессов и защищенность информационных ресурсов, а также основные направления и методы воздействия на персонал с целью повышения ИБ.

3.5. Политика ИБ разрабатывается для того, чтобы обеспечить выбор

адекватных и пропорциональных средств управления информационной безопасностью, которые защищают информационные активы и придают уверенность заинтересованным сторонам.

3.6. Политика ИБ дает ясное представление о требуемом поведении пользователей, администраторов и других работников Института при внедрении и использовании информационных систем и средств защиты информации, при осуществлении информационного обмена и выполнении операций по обработке информации, а также защита самих пользователей (сотрудников института, его клиентов и контрагентов).

3.7. Политика ИБ является общедоступным документом, который может предоставляться без ограничений всем заинтересованным сторонам.

4. Цели, задачи и принципы обеспечения информационной безопасности

4.1. Основными целями обеспечения ИБ являются:

- создание и укрепление системы защиты информации института;
- обеспечение направления и поддержки со стороны руководства МТИИ для защиты информации в соответствии с требованиями, а также законами и нормами в области ИБ;
- защита информационных ресурсов, а также прав человека и интересов института в информационной сфере;
- повышение деловой репутации и корпоративной культуры института.

4.2. Основными задачами, решаемыми при проведении политики ИБ института, являются:

- совершенствование нормативных внутренних документов института в соответствии с законодательством Республики Казахстан (далее - РК) в области ИБ;
- выявление, оценка, прогнозирование источников угроз ИБ. определение параметров доступности защищаемых объектов;
- координация деятельности структурных подразделений МТИИ в области обеспечения ИБ;
- организация мероприятий по строгому и неукоснительному соблюдению режимов учёта авторизации и аутентификации сотрудников:
- постоянный контроль и аудит всех доступных объектов информационной структуры, в том числе с целью включения их в информационную среду и организации их дальнейшей защиты;
- обеспечение активного участия института в процессах создания и использования глобальных информационных сетей и систем;
- оптимизация существующей информационной инфраструктуры института и прогнозирование её развития с учётом требований поддержания ИБ на максимальном уровне при оптимальных затратах.

4.3. При достижении поставленных целей МТИИ намерен руководствоваться следующими принципами:

- вовлеченность высшего руководства института в процесс обеспечения ИБ. Деятельность по обеспечению ИБ инициирована и контролируется руководством

института. Руководство института выполняет те же правила по обеспечению ИБ, что и все работники;

- законность обеспечения ИБ. Институт реализует меры обеспечения ИБ в строгом соответствии с действующим законодательством и договорными обязательствами;

- согласованность действий по обеспечению информационной, физической и экономической безопасности. Действия по обеспечению информационной, физической и экономической безопасности осуществляются на основе четкого взаимодействия заинтересованных подразделений МТИИ и согласованы между собой по целям, задачам, принципам, методам и средствам;

- экономическая целесообразность. институт стремится выбирать меры обеспечения ИБ с учетом затрат на их реализацию, вероятности возникновения угроз ИВ и объема возможных потерь от их реализации;

- знание своих работников. Институт стремится тщательно подбирать персонал (работников), вырабатывать и поддерживать корпоративную этику, что создает благоприятную среду для деятельности и снижает риски ИБ;

- документированность требований ИБ. Институт стремится, чтобы все требования в области ИБ были зафиксированы во внутренних нормативных документах утвержденных руководством;

- осведомленность в вопросах обеспечения ИБ. Документированные требования в области ИБ доводятся до сведения работников института. Институт на периодической основе осуществляет информирование. обучение работников по вопросам обеспечения ИБ;

- реагирование на инциденты ИБ. Институт стремится выявлять, у читывать и оперативно реагировать на действительные, предпринимаемые и вероятные нарушения ИБ;

- персональная ответственность. Работники института несут персональную ответственность за соблюдение требований ИБ.

Обязанности по обеспечению ИБ включаются в трудовые договоры и должностные инструкции работников.

5. Объекты, угрозы, методы, средства и основные направления обеспечения информационной безопасности института

5.1. К объектам информационной безопасности относятся:

- права физических и юридических лиц на получение, распространение и использование информации, защиту конфиденциальной информации и интеллектуальной собственности;

- информационные ресурсы вне зависимости от форм хранения, содержащие сведения, составляющие государственные секреты, коммерческую тайну и другую конфиденциальную информацию, а также открытую (общедоступную) информацию;

- система формирования, хранения, распространения и использования информационных ресурсов, включающая в себя информационные системы различного класса и назначения, библиотеки, архивы, базы и банки данных, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, научно-технический и обслуживающий

персонал;

- система формирования общественного сознания (мировоззрение, политические взгляды, моральные ценности и прочие), базирующаяся на средствах массовой информации и пропаганды;
- сети телекоммуникаций специального назначения, а также спутниковые системы связи;
- средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение), автоматизированные системы управления, системы связи и передачи данных, осуществляющие прием, обработку, хранение и передачу информации.

5.2. Понятия и структура ИС МТИИ. ИС института, является организационно - технической системой, в которой реализуются информационные технологии, и предусматривается использование аппаратного, программного и других видов обеспечения, необходимого для реализации информационных процессов сбора, обработки, накопления, хранения, поиска и распространения информации.

5.3. Основу ИС института составляют территориально распределенные компьютерные системы (вычислительные сети), элементы которых расположены на разных этажах здания и связаны между собой транспортной средой, которая использует физические принципы ("витая пара", оптико-волоконные каналы, радиоканал и т.п.). Основу аппаратных (технических) средств таких систем составляют ЭВМ (группы ЭВМ), периферийные, вспомогательные устройства и средства связи, сопрягаемые с ЭВМ. Состав программных средств определяется возможностями ЭВМ и характером решаемых задач в данной ИС.

5.4. Основными элементами, составляющими такую систему, являются;

- локальная сеть;
- каналы и средства связи;
- узлы коммутации;
- рабочие места сотрудников ИС;
- учебные лаборатории;
- рабочее место удаленного пользователя;
- носители информации (магнитные, оптические и др.);
- отдельные ПК и рабочие станции;
- непосредственно пользователи (работники и обучающиеся МТИИ).

5.5. Перечисленные элементы в процессе функционирования, активно взаимодействую между собой, что в свою очередь позволяет использовать различные точки доступа к информационным ресурсам: это библиотека, компьютерные классы, кафедральные компьютерные сети, и, наконец, система доступа студентов и преподавателей института с домашних компьютеров (удаленных компьютеров). Такое количество точек доступа к ИР. в значительной степени повышает проблему безопасности.

5.6. При формировании политики безопасности, соответствующие структурные подразделения МТИИ, должны осуществлять комплексный подход к защите ИС. Комплексный подход подразумевает использование единой

совокупности законодательных, организационных и технических мер, направленных на выявление, отражение и ликвидации различных видов угроз ИБ.

5.7. Все имеющиеся у МТИИ информационные объекты (и соответствующие элементы информационной инфраструктуры), могут быть разделены на пять или шесть основных групп по уровню своей значимости и конфиденциальности:

5.7.1. Государственная и/или критически важная (абсолютно секретная) информация - информация, требующая особых гарантий безопасности. МТИИ, владеет значительным объемом информации, относящейся к передовым направлениям науки и техники, используемой как при подготовке специалистов, так и при выполнении научно-исследовательских работ. Обращение с этими сведениями требует особого режима, исключающего допуск сторонних лиц.

5.7.2. Важная информация (информация, составляющая коммерческую тайну) - информация, составляющая коммерческую тайну МТИИ (секретам производства), принадлежащие институту на законных основаниях сведения любого характера (производственные, технические, финансово-экономические, организационные и другие). в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности при условии, что:

- эти сведения имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам;
- к этим сведениям нет свободного доступа на законном основании;

институт принимает надлежащие меры (правовые, организационные, технические) к охране их конфиденциальности, т.е. вводит режим коммерческой тайны.

5.7.3. Не может быть установлен режим коммерческой тайны в отношении следующих сведений:

- содержащихся в учредительных документах МТИИ;
- содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
- о состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке;
- о численности, о составе работников, о системе оплаты и условиях труда, о наличии свободных рабочих мест;
- о нарушениях законодательства Республики Казахстан и фактах привлечения к ответственности за совершение этих нарушений;
- о перечне лиц, имеющих право действовать без доверенности от имени юридического лица, используемая только внутри института, нарушение конфиденциальности которой может нанести серьезный ущерб самому МТИИ или его партнерам.

5.8. Эти сведения принято называть служебной и/или коммерческой тайной. К ним относятся:

5.8.1. Общие сведения:

- протоколы заседаний ученого Совета МТИИ или его отдельные положения, а также материалы по вопросам повестки дня заседаний (кроме материалов, которые необходимо размещать на сайте общества в соответствии с

требованиями устава);

- сведения о штатной численности института;
- сведения имеющих баз данных;
- сведения о тактике переговоров с деловыми партнерами.

5.8.2. Сведения финансово-экономической сферы:

- сведения о планируемых инвестициях института;
- сведения об отдельных финансовых операциях и доходах по этим операциям;
- сведения о ценовой политике и доходах по этим операциям:
- планируемые решения о создании юридических лиц или участия в них;
- фактические состояние расчетов с теми или иными партнерами;
- сведения о производственных, коммерческих и финансовых отношениях с партерами;
- условия любых договоров, заключаемых институтом;
- планируемые рекламные акции;
- отчетность и другая информация о финансово-хозяйственной деятельности института, за исключением сведения, публикуемых в официальном порядке в средствах массовой информации.

5.8.3. Информация социальной сферы института:

- персональные данные работников;
- интеллектуальный потенциал коллектива, его специалисты, их моральные и деловые качества, наличие компрометирующих их сведений, биографические данные;
- используемая в коллективе система оплаты труда, система стимулов, укрепляющих дисциплину, повышающих производительность труда, сохранность коммерческой тайны;
- кадровая статистика;
- любые возможности нанесения морального ущерба институту, понижение его престижа в обществе и конкурентоспособности.

5.8.4. Безопасность МТИИ:

- сведения о порядке и состоянии организации охраны, пропускном режиме, системе сигнализации, шифрах;
- данные об информационной системе и о применяемых способах информационной защиты.

5.8.5. Профессиональная/значимая (конфиденциальная) информация - информация, предназначенная для использования ограниченным кругом сотрудников и руководителей института:

- персональная информация - информация о сотрудниках, не подлежащая разглашению: персональные данные – любая документированная и/или занесенная на машинные носители информация, которая относится к конкретному человеку и/или которая может быть отождествлена с конкретным человеком. Это информация о студентах, о преподавателях, партнерах и др;
- информация для внутреннего использования - информация для использования внутри института, нарушение конфиденциальности которой не может нанести вреда;
- прочая информация - открытая информация, конфиденциальность которой не имеет особого значения для деятельности МТИИ;

- доступ к общедоступной информации является открытым и ее использование не может нанести вреда ИС;

- доступ к информации ограниченного доступа строго регламентирован, т.е. четко установлено, где, кем, в каком объеме и на каких условиях может быть осуществлено использование данной информации. Данное разграничение должно обуславливаться тем, что пользователи ИС института имеют различные профессиональные интересы и уровень подготовки при работе с информацией различного рода. Это преподаватели, занятые постановкой новых лекционных курсов, лабораторных и исследовательских практикумов; сотрудники, ведущие исследовательские и проектные разработки; сотрудники финансово-экономического управления, отдела бухгалтерского учета и отчетности, административно-правовой службы, отдела организационной и кадровой работы, отдела офис-регистратора, отдел учета студентов и производственной практики, учебного отделов, библиотеки и т.п., а также студенты.

5.9. Из этого следует, что информация ограниченного доступа должна подвергаться защите от воздействия различных событий, явлений, как внутренних, так и внешних, способных в той или иной мере нанести ущерб данной информации.

5.10. Помимо разграничения прав доступа и определения других мер по защите циркулирующей в институте информации, в целом эффективность защиты информации в ИС достигается лишь в том случае, если обеспечивается ее надежность на всех объектах и элементах системы, которые могут быть подвергнуты угрозам со стороны дестабилизирующих факторов.

5.11. В МТИИ к таким информационным объектам (коммерческая тайна) применяются:

- специальные требования к резервному копированию информации (такие как более высокая частота резервного копирования и использование более надежных носителей для этого);

- специальные требования к идентификации и аутентификации пользователей (такие как комбинирование биометрической идентификации и идентификации при помощи паролей):

- специальные требования к копировально-множительной технике, используемой для работы с конфиденциальной информацией;

- специальные требования к помещениям, в которых проводятся совещания по секретной тематике и обрабатывается соответствующая информация (толщина и материал стен, расположение помещений в зданиях, защищенность окон, надежность дверей и запоров, а также охранной и пожарной сигнализации, обследования на предмет выявления подслушивающих устройств и т.п.) и другие.

5.12. В МТИИ к Политике ИБ, относящиеся к определенным аспектам использования информационных технологий, организации информационных потоков и организации работы персонала (профессиональная. персональная. информации, информация для внутреннего пользования, прочие информации) - применяются:

- правила опубликования открытых информационных материалов, в том числе политика организации веб-сайта МТИИ (в части предотвращения возможных утечек и искажений информации);

- правила использования сети Интернет (в части предотвращения

возможных утечек информации);

- правила использования отдельных информационных и коммуникационных технологий института, удаленного доступа к корпоративными информационным системам, а также использования личных компьютеров сотрудников в служебных целях;
- классификации информационных систем, информационных ресурсов и объектов информации с точки зрения их значимости и усилий, которые необходимо предпринимать для их защиты;
- правила приобретения, установки, модификации и обновления программного обеспечения, а также аутсорсинга разработки и проектирования программного обеспечения;
- правила закупки аппаратных средств информационных систем, систем информационной безопасности;
- правила использования пользователями собственного программного обеспечения (т.е., ПО, самостоятельно разрабатываемого институтом);
- общие для всего института правила использования паролей и других средств персональной идентификации;
- правила использования электронно-цифровой подписи и инфраструктуры публичных ключей;
- правила обеспечения внутри объектового режима и физической защищенности информационных активов;
- правила доступа к внутренним информационным ресурсам сторонних пользователей (организаций);
- общий для всего института порядок привлечения к ответственности за нарушение определенных правил информационной безопасности.

5.13. В целях охраны конфиденциальности информации работник обязан:

- в соответствии с нормами Трудового законодательства письменно предоставить согласие на обработку персональных данных, в том числе выполнять установленный в институте работодателем режим коммерческой тайны;
- не разглашать информацию, составляющую коммерческую тайну: обладателями, которой являются институт и его контрагенты, и без их согласия не использовать эту информацию в личных целях;
- передать институту при прекращении или расторжении трудового договора, имеющиеся в пользовании работника материальные носители информации, содержащие сведения, составляющие коммерческую тайн). Институт также имеет право осуществлять обработку персональных данных Обучающегося на основании согласия самого Обучающегося в соответствии с Законодательством РК.

5.14. Нарушение конфиденциальности информации влечет за собой дисциплинарную, гражданско-правовую, административную или уголовную ответственность в соответствии с законодательством РК.

5.15. Работник, который в связи с исполнением трудовых обязанностей получил доступ к информации, составляющей коммерческую тайну института, в случае умышленного или неосторожного разглашения этой информации при отсутствии в действиях такого работника состава преступления несет дисциплинарную ответственность в соответствии с законодательством РК.

5.16. Возмещение убытков, причиненных институту в связи с нарушением как прав института на ею коммерческую тайну, производится в установленном законодательством РК порядке, организациями и лицами (в том числе работниками института), нарушившими указанные права. При этом ответственность несут также работники и должностные лица института, не выполнившие или не обеспечившие выполнение требований настоящего положения и тем самым способствовавшие нарушению, а также не принимавшие необходимых и достаточных мер по пресечению ставших им известными фактов нарушения прав института.

6. Ответственность

6.1. Ответственность за проведение политики ИБ формируется на основании следующих правил:

- ответственность распространяется по принципу соподчинённое™ подразделений института, имеет иерархическую структуру: ответственность за вышележащие информационные объекты не может быть возложена на нижележащие структуры, и наоборот ответственность за нижележащие объекты может быть возложена на вышестоящие структуры. - вся полнота ответственности лежит на ректоре МТИИ, который, по своему усмотрению и по своей доверенности, может распределять эту ответственность на остальных сотрудников;
- соблюдение политики ИБ является непременным условием действующего трудового договора и должностных обязанностей сотрудника;
- сотрудник не может отказаться от возложенных на него права и обязанности следовать политике ИБ. за исключением случаев, противоречащих действующему законодательству РК;
- ответственность за нарушение политики ИБ возникает вне зависимости от умысла;
- тяжесть ответственности за нарушение политики ИБ определяется ректором института и не может противоречить действующему законодательству.

6.2. Гражданско-правовая ответственность является одним из видов юридической ответственности и характеризуется применением к нарушителю предусмотренных законом или договором мер воздействия, влекущих для него отрицательные, экономически невыгодные последствия имущественного характера.

6.3. Договоры, разрешающие доступ третьей стороне (сотрудники, осуществляющие поддержку и сопровождение аппаратных средств и программного обеспечения, осуществляющие уборку, питание, охрану, уборку и др. услуги; лица, работающие по трудовым соглашениям, консультанты) должны включать процедуру определения прав и условий доступа других лиц.