УТВЕРЖДАЮ
И.о. ректора

_____Ю.С. Клочков
«_____» _____ 20___г.

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 22951055844CB6521B4706EEB4A4C9F6
Владелец: Клочков Юрий Сергеевич
Действителен: с 16.05.2024 до 09.08.2025

СОДЕРЖАНИЕ

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящая политика информационной безопасности (далее - политика) является декларацией руководства федерального государственного бюджетного образовательного учреждения высшего образования «Тюменский индустриальный университет» (далее - ТИУ) о намерениях и направлениях деятельности ТИУ в области информационной безопасности, а также об обязательствах выполнять требования, связанные с информационной безопасностью и поддерживать постоянное совершенствование видов деятельности, связанных с системой управления информационной безопасностью.

1.2. Руководство ТИУ демонстрирует свое лидерство и приверженность в отношении системы управления информационной безопасностью в ТИУ:

1.2.1. Установлением настоящей политики и целей информационной безопасности, совместимых со стратегическим направлением развития ТИУ;

1.2.2. Интеграцией требований системы управления информационной безопасности в процессы ТИУ;

1.2.3. Доступностью ресурсов, необходимых для системы управления информационной безопасности;

1.2.4. Декларированием важности обеспечения эффективного управления информационной безопасностью и соответствия требованиям системы управления информационной безопасности;

1.2.5. Направляя и поддерживая лиц, способствующих повышению результативности системы управления информационной безопасности;

1.2.6. Постоянным улучшением системы управления информационной безопасности.

1.3. Информационная безопасность ТИУ – состояние защищенности ТИУ от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод работников, обучающихся и других заинтересованных лиц, реализация всех видов деятельности ТИУ в защищенном информационном пространстве в соответствии с законодательством РФ в области информационной безопасности, технологический суверенитет и устойчивое развитие ТИУ, сохранение конфиденциальности, целостности и доступности защищаемых информационных активов ТИУ.

1.4. Настоящая политика соответствует целям деятельности ТИУ, содержит цели информационной безопасности и обязательство соответствовать применимым требованиям, относящимся к информационной безопасности.

1.5. Настоящая политика разработана в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне», Указом Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», Постановлением правительства Российской Федерации от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственного за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)» и иными нормативно-правовыми актами, устанавливающими требования к обеспечению информационной безопасности, Программой развития федерального государственного бюджетного образовательного учреждения высшего образования «Тюменский индустриальный университет» на 2023-

2032 годы, Корпоративным кодексом работников федерального государственного бюджетного образовательного учреждения высшего образования «Тюменский индустриальный университет», Программой «Обеспечение комплексной безопасности Тюменского индустриального университета на 2020-2024 гг.» и иными локальными нормативными актами ТИУ, национальным стандартом РФ ГОСТ Р ИСО/МЭК 27001-2021 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования», утв. приказом Федерального агентства по техническому регулированию и метрологии от 30.11.2021 № 1653-ст, национальным стандартом РФ ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности», утв. приказом Федерального агентства по техническому регулированию и метрологии от 20.05.2021 № 416-ст, национальным стандартом РФ ГОСТ Р ИСО/МЭК 27003-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации», утв. приказом Федерального агентства по техническому регулированию и метрологии от 19.05.2021 № 387-ст.

1.6. Настоящая политика:

1.6.1. Является публичной и размещается на сайте ТИУ;

1.6.2. Доводится до сведения всех работников и обучающихся ТИУ;

1.6.3. Положение об ознакомлении с настоящей политикой и ответственностью за нарушения ее требований вместе со ссылкой на место ее размещения на сайте ТИУ вносится в документы, обуславливающие возникновение обязательств между ТИУ и заинтересованными сторонами.

2. ОБЛАСТЬ ДЕЙСТВИЯ

2.1. Настоящая политика распространяется и влияет на все виды деятельности ТИУ, на всю обрабатываемую в ТИУ информацию, на любые информационные системы и ресурсы, средства обработки информации, а также на всех работников и обучающихся ТИУ, а также заинтересованных лиц (включая контрагентов, лиц, работающих по договорам гражданско-правового характера и других лиц).

2.2. Обработка информации - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с информацией, включая сбор, запись, систематизацию, накопление, хранение, обновление, изменение, извлечение, использование, передачу (распространение, предоставление), блокирование, удаление, уничтожение информации в любой форме.

2.3. Настоящая политика распространяется и влияет на все формы представления информации – электронную, на бумажных носителях, устную (речевую), визуальную, электромагнитную и другие формы.

3. ЦЕЛИ

3.1. Целью настоящей политики является установление обязательных требований к поведению и практической деятельности, связанными с информационной безопасностью, и к обязательствам ТИУ в этой области.

3.2. Цели ТИУ в области информационной безопасности:

3.2.1. Разработка и внедрение в деятельность всесторонней системы управления информационной безопасностью, соответствующей требованиям законодательства РФ в области информационной безопасности, в частности, в области обеспечения безопасности

критической информационной инфраструктуры, персональных данных, защиты государственной, служебной, коммерческой и иных видов тайн;

3.2.2. Обеспечение противодействия техническим разведкам и технической защиты информации;

3.2.3. Исключение или существенное снижение негативных последствий (ущерба) в отношении ТИУ, повышение защищенности ТИУ от возможного нанесения ему материального, репутационного или иного ущерба вследствие нарушения информационной безопасности ТИУ.

3.2.4. Повышение деловой репутации и корпоративной культуры ТИУ.

4. ПРИНЦИПЫ

4.1. Информационная безопасность обеспечивается в ТИУ на основе принципов:

4.1.1. Законности;

4.1.2. Признания, соблюдения и защиты прав и свобод человека и гражданина;

4.1.3. Сотрудничества и взаимопонимания;

4.1.4. Персональной ответственности;

4.1.5. Экономической целесообразности;

4.1.6. Участия руководства ТИУ в процессе обеспечения информационной безопасности.

5. КЛЮЧЕВЫЕ РЕЗУЛЬТАТЫ

5.1. Ключевыми результатами, определяющими достижение ТИУ целей в области информационной безопасности являются:

5.1.1. Обеспечение конфиденциальности, целостности и доступности защищаемых информационных ресурсов ТИУ.

5.1.2. Своевременное выявление угроз безопасности информации и уязвимостей информационных систем, программных и программно-аппаратных средств.

5.1.3. Предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации).

5.1.4. Поддержание стабильной деятельности ТИУ и его производственных процессов в случае проведения компьютерных атак.

5.1.5. Установление ответственности за управление и использование информационных ресурсов ТИУ.

5.1.6. Разработка и внедрение локальных нормативных актов, регулирующих отношения в сфере информационной безопасности в ТИУ, охватывающих областью действия все аспекты функционирования системы управления информационной безопасности ТИУ.

5.1.7. Поддержание достаточного уровня осведомленности работников и обучающихся ТИУ и их понимания рисков, связанных с информационной безопасностью.

6. ОТВЕТСТВЕННОСТЬ

6.1. Соблюдение требований и правил в области информационной безопасности является обязательным для всех работников и обучающихся ТИУ, а также заинтересованных лиц.

6.2. Нарушения в области информационной безопасности ТИУ подлежат внутреннему расследованию.

6.3. Лица, виновные в нарушении требований информационной безопасности, несут дисциплинарную, гражданско-правовую, административную и уголовную ответственность в соответствии с законодательством Российской Федерации.

6.4. Руководство ТИУ назначает обязанности и полномочия для ролей, имеющих отношение к обеспечению информационной безопасности, доведение этих обязанностей и полномочий до всех заинтересованных сторон и осуществляет общий контроль за состоянием системы управления информационной безопасности.

6.5. Руководство ТИУ проводит проверку системы управления информационной безопасности через запланированные интервалы времени в целях обеспечения уверенности в сохраняющейся ее приемлемости, адекватности и результативности.

7. ТРЕБОВАНИЯ

7.1. Для обеспечения информационной безопасности ТИУ применяет правовые, организационно-технические, криптографические и иные меры защиты.

7.2. Основными требованиями в области информационной безопасности ТИУ являются:

7.2.1. Организация деятельности по информационной безопасности

7.2.1.1. Определение и распределение всех обязанностей по обеспечению информационной безопасности.

7.2.1.2. Определение областей, за которые работники несут ответственность. В частности:

а) идентификация и описание активов и процессов информационной безопасности;

б) назначение ответственных лиц с возложением ответственности для каждого актива или процесса информационной безопасности;

в) определение и документирование уровней полномочий;

г) определение и документирование аспектов взаимодействия и контроля информационной безопасности при взаимодействии с поставщиками.

7.2.1.3. Разделение пересекающихся обязанностей и зон ответственности для уменьшения возможности несанкционированного или непреднамеренного изменения или нецелевого использования активов ТИУ.

7.2.1.4. Определение и внедрение процесса оценки и обработки рисков информационной безопасности через запланированные интервалы времени или в случае предполагаемых или произошедших существенных изменений.

7.2.1.5. Поддержание соответствующих контактов с уполномоченными органами власти.

7.2.1.6. Поддержание соответствующего взаимодействия с заинтересованными профессиональными сообществами и ассоциациями или форумами, проводимыми специалистами по безопасности.

7.2.1.7. Рассмотрение требований информационной безопасности при управлении проектами независимо от типа проекта.

7.2.1.8. Реализация поддерживающих мер обеспечения информационной безопасности для управления рисками информационной безопасности, связанными с использованием мобильных устройств.

7.2.1.9. Реализация поддерживающих мер безопасности для защиты информации, доступ к которой, обработку или хранение осуществляют в местах дистанционной работы.

7.2.2. Информационная безопасность, связанная с персоналом

7.2.2.1. Проверка всех кандидатов при приеме на работу согласно соответствующим законам, правилам и этическим нормам соразмерно категории информации, которая

доступна работнику по должности, и предполагаемым рискам информационной безопасности.

7.2.2.2. Установление в договорах, соглашениях с работниками и подрядчиками их обязанностей, а также обязанностей ТИУ по обеспечению информационной безопасности.

7.2.2.3. Требование от всех работников, обучающихся и заинтересованных лиц соблюдения требований информационной безопасности.

7.2.2.4. Повышение осведомленности всех работников и обучающихся ТИУ в области информационной безопасности, уведомление заинтересованных лиц об обновлениях требований информационной безопасности ТИУ.

7.2.2.5. Привлечение к установленной законодательством РФ ответственности лиц, совершивших нарушения требований информационной безопасности.

7.2.2.6. Определение, юридическое оформление и доведение до работников, обучающихся и заинтересованных лиц ответственности и обязанностей, относящихся к информационной безопасности, которые сохраняются после увольнения, прекращения договорных отношений либо перевода.

7.2.3. Управление информационными активами

7.2.3.1. Идентификация и инвентаризация информации, информационных систем и ресурсов, средств обработки информации и других активов, связанных с информацией, поддержание перечня этих активов в актуальном состоянии.

7.2.3.2. Определение владельца для каждого актива, включенного в перечень инвентаризации.

7.2.3.3. Идентификация, документальное оформление и реализация правил допустимого использования информационных активов, включая информацию и средства ее обработки.

7.2.3.4. Возвращение всеми работниками и внешними пользователями всех активов ТИУ, находящихся в их пользовании, после увольнения, истечения срока действия договора или соглашения.

7.2.3.5. Категорирование информации с точки зрения нормативных правовых требований, ценности, критичности и чувствительности к неавторизованному раскрытию или модификации.

7.2.3.6. Разработка и реализация соответствующего набора процедур маркировки информации в соответствии с принятой в РФ и ТИУ системой категорирования информации.

7.2.3.7. Разработка и реализация процедуры обращения с информационными активами в соответствии с принятой в РФ и ТИУ системой категорирования информации.

7.2.3.8. Реализация процедуры по управлению сменными носителями информации в соответствии с принятой в РФ и ТИУ системой категорирования информации.

7.2.3.9. Надежная и безопасная утилизация носителей информации при выводе их из эксплуатации.

7.2.3.10. Защита во время транспортировки от несанкционированного доступа, ненадлежащего использования или повреждения носителей информации, содержащих защищаемую информацию.

7.2.4. Управление доступом

7.2.4.1. Регламентация и документирование процесса управления доступом.

7.2.4.2. Предоставление пользователям доступа только к тем сетям и сетевым сервисам, на использование которых они получили конкретное разрешение.

7.2.4.3. Реализация формализованного процесса регистрации и отмены регистрации пользователей для назначения прав доступа.

7.2.4.4. Реализация формализованного процесса назначения или отмены прав доступа пользователей к системам и сервисам.

7.2.4.5. Ограничение и контроль распределения и использования привилегированных прав доступа.

7.2.4.6. Регулярный пересмотр прав доступа пользователей владельцами информационных активов.

7.2.4.7. Аннулирование после увольнения, истечения срока действия договора или соглашения, либо корректировка в случае необходимости прав доступа всех работников, обучающихся и внешних пользователей к информации и средствам ее обработки.

7.2.4.8. Использование аутентификационной информации пользователями в строгом соответствии с установленными в ТИУ требованиями информационной безопасности.

7.2.4.9. Ограничение в соответствии с требованиями по управлению доступом доступа к информации и функциям прикладных систем.

7.2.4.10. Управление посредством безопасной процедуры входа в систему в соответствии с требованиями по управлению доступом доступа к системам и приложениям.

7.2.4.11. Реализация интерактивной системы управления паролями обеспечивающей уверенность в качестве паролей.

7.2.4.12. Ограничение и строгий контроль использования служебных программ, которые могут обойти меры и средства информационной безопасности систем и приложений.

7.2.4.13. Ограничение доступа к исходному коду программ.

7.2.5. Криптография

7.2.5.1. Разработка формализованной процедуры использования средств криптографической защиты информации.

7.2.5.2. Регламентация требований, определяющих использование, защиту и срок действия криптографических ключей, применяющихся на протяжении всего их жизненного цикла.

7.2.6. Физическая безопасность и защита от воздействия окружающей среды

7.2.6.1. Определение и использование периметров безопасности (контролируемых зон) для защиты зон, содержащих информацию ограниченного доступа и средств ее обработки.

7.2.6.2. Защита зон безопасности соответствующими мерами и средствами контроля доступа.

7.2.6.3. Физическая защита зданий, помещений и оборудования.

7.2.6.4. Физическая защита от стихийных бедствий, злоумышленных атак или аварий.

7.2.6.5. Контроль мест доступа, таких, как зоны погрузки и разгрузки, и других мест, где неуполномоченные лица могут проникать в помещения, и, по возможности, изоляция их от средств обработки информации, во избежание несанкционированного доступа к ним.

7.2.6.6. Размещение и защита оборудования таким образом, чтобы снизить риски информационной безопасности от угроз и опасностей со стороны окружающей среды и возможности несанкционированного доступа.

7.2.6.7. Защита оборудования от сбоев электропитания и других сбоев, вызванных отказами в предоставлении вспомогательных услуг.

7.2.6.8. Защита от перехвата информации, помех или повреждения помещений, в которых обрабатывается информация ограниченного доступа, технических средств обработки информации, вспомогательных технических средств и систем, кабелей питания и телекоммуникационных кабелей, используемых для передачи данных или для поддержки информационных сервисов.

7.2.6.9. Проведение технического обслуживания оборудования, для обеспечения его непрерывной доступности и целостности.

7.2.6.10. Исключение без предварительного разрешения выноса оборудования, информации или программного обеспечения за пределы площадки эксплуатации.

7.2.6.11. Обеспечение безопасности информационных активов вне помещений ТИУ, учитывая различные риски информационной безопасности, связанные с работой вне помещений.

7.2.6.12. Проверка всех компонентов оборудования, содержащих носители данных, с целью обеспечения уверенности, что вся защищаемая информация и лицензионное программное обеспечение были удалены или перезаписаны безопасным образом до утилизации или повторного использования этих компонентов оборудования.

7.2.6.13. Обеспечение пользователями соответствующей защиты оборудования, оставленного без присмотра.

7.2.6.14. Использование политики «чистого стола» в отношении документов на бумажных носителях и сменных носителей информации, а также политики «чистого экрана» для средств обработки информации.

7.2.7. Информационная безопасность при эксплуатации

7.2.7.1. Документирование и доступность всем нуждающимся в них пользователям эксплуатационных процедур.

7.2.7.2. Управление изменениями в ТИУ, средствах обработки информации и системах, влияющих на информационную безопасность.

7.2.7.3. Мониторинг, корректировка и прогнозирование использования информационных ресурсов исходя из будущих требований к производительности системы.

7.2.7.4. Разделение сред разработки, тестирования и эксплуатации для снижения рисков несанкционированного доступа или изменений среды эксплуатации.

7.2.7.5. Реализация мер обеспечения информационной безопасности, связанных с обнаружением, предотвращением и восстановлением, в сочетании с соответствующим информированием пользователей для защиты от вредоносных программ.

7.2.7.6. Регулярное создание и проверка резервных копий информации, программного обеспечения и образов системы.

7.2.7.7. Формирование, ведение и регулярный анализ регистрационных журналов, фиксирующих действия пользователей, нештатные ситуации, ошибки и события безопасности.

7.2.7.8. Защита средств регистрации и информации регистрационных журналов от фальсификации и несанкционированного доступа.

7.2.7.9. Регистрация действий системных администраторов и операторов систем, защита и регулярный анализ регистрационных журналов.

7.2.7.10. Синхронизация часов всех систем обработки информации в рамках ТИУ или домена безопасности будут синхронизироваться с единым эталонным источником времени.

7.2.7.11. Реализация процедур контроля установки программного обеспечения в системах, находящихся в эксплуатации.

7.2.7.12. Своевременное получение информация о технических уязвимостях используемых информационных систем, оценка подверженности ТИУ таким уязвимостям и принятие соответствующих мер в отношении связанного с этим риска информационной безопасности.

7.2.7.13. Реализация правил, регулирующих установку программного обеспечения пользователями.

7.2.7.14. Планирование и реализация процесса регистрации событий [аудита] и деятельности, связанной с контролем находящихся в эксплуатации систем, для минимизации сбоев.

7.2.8. Информационная безопасность коммуникаций

7.2.8.1. Управление и контроль сетями для обеспечения защиты информации в системах и приложениях.

7.2.8.2. Идентификация и включение в соглашения по сетевым сервисам независимо от того, будут ли они обеспечиваться силами ТИУ или осуществляться с использованием аутсорсинга механизмов обеспечения безопасности, уровней обслуживания и требований к управлению для всех сетевых сервисов.

7.2.8.3. Разделение групп информационных сервисов, пользователей и информационных систем в сети.

7.2.8.4. Реализация процедур передачи информации, а также соответствующих мер, обеспечивающих безопасность информации, передаваемой с использованием всех видов средств связи.

7.2.8.5. Реализация процедуры безопасной передачи деловой информации между ТИУ и внешними сторонами.

7.2.8.6. Реализация защиты информации при электронном обмене сообщениями.

7.2.8.7. Идентификация, документальное оформление и регулярный пересмотр соглашений о конфиденциальности или неразглашении, отражающих потребности ТИУ в обеспечении защиты информации.

7.2.9. Приобретение, разработка и поддержка информационных систем

7.2.9.1. Включение требований, относящихся к информационной безопасности, в перечень требований для новых информационных систем или для усовершенствования существующих информационных систем.

7.2.9.2. Защита информации, используемой в прикладных сервисах и передаваемой по сетям общего пользования, от мошеннической деятельности, оспаривания договоров, а также несанкционированного раскрытия и модификации.

7.2.9.3. Защита информации, используемой в транзакциях прикладных сервисов, для предотвращения неполной передачи, ложной маршрутизации, несанкционированного изменения, раскрытия, дублирования или воспроизведения сообщений.

7.2.9.4. Реализация процедуры безопасной разработки программного обеспечения и систем в рамках ТИУ.

7.2.9.5. Проверка и тестирование критически важных для деятельности ТИУ приложений при внесении изменений в операционные платформы, чтобы обеспечить уверенность в отсутствии неблагоприятного воздействия на деятельность или безопасность ТИУ.

7.2.9.6. Установка, документирование, поддержка и применение к любым работам по реализации информационных систем принципов безопасного проектирования систем.

7.2.9.7. Реализация процедуры защиты безопасных сред разработки, используемых для разработки и интеграции систем на всех стадиях жизненного цикла разработки системы.

7.2.9.8. Осуществление надзора за разработкой систем, выполняемой подрядчиками, и ее мониторинг.

7.2.9.9. Тестирование функциональных возможностей безопасности в процессе разработки.

7.2.9.10. Реализация программы приемо-сдаточных испытаний и установления связанных с ней критериев для новых информационных систем, обновлений и новых версий.

7.2.9.11. Тщательный выбор, защита и контроль тестовых данных.

7.2.10. Взаимоотношения с поставщиками

7.2.10.1. Согласование с поставщиками и документирование требований информационной безопасности, направленных на снижение рисков, связанных с доступом поставщиков к информационным активам организации.

7.2.10.2. Установление и согласование соответствующих требований по информационной безопасности с каждым поставщиком, который может получить доступ к информации ТИУ, обрабатывать, хранить, передавать информацию или предоставлять соответствующие компоненты ИТ-инфраструктуры.

7.2.10.3. Включение в соглашения с поставщиками требований по рассмотрению рисков информационной безопасности, связанных с цепочкой поставок продуктов и услуг информационно-коммуникационных технологий.

7.2.10.4. Регулярный мониторинг, проверка и аудит деятельности поставщиков по предоставлению услуг.

7.2.11. Управление инцидентами информационной безопасности

7.2.11.1. Реализация процесса управления реагированием на инциденты информационной безопасности.

7.2.11.2. Обязанность пользователей незамедлительно сообщать о событиях информационной безопасности по соответствующим каналам управления.

7.2.11.3. Обязанность работников, обучающихся и заинтересованных лиц, использующих информационные системы и услуги ТИУ, обращать внимание на любые замеченные или предполагаемые недостатки информационной безопасности в системах или сервисах и сообщать о них.

7.2.11.4. Оценка событий безопасности и принятие решения, следует ли их классифицировать как инциденты информационной безопасности.

7.2.11.5. Реализация процесса реагирование на инциденты информационной безопасности.

7.2.11.6. Использование знаний, приобретенных в результате анализа и урегулирования инцидентов информационной безопасности, для уменьшения вероятности или влияния будущих инцидентов.

7.2.11.7. Реализация процесса идентификации, сбора, получения и сохранения информации, которая может использоваться в качестве свидетельств.

7.2.12. Аспекты информационной безопасности в рамках управления непрерывностью деятельности

7.2.12.1. Определение требований к информационной безопасности и менеджменту непрерывности информационной безопасности при неблагоприятных ситуациях, например во время кризиса или бедствия.

7.2.12.2. Установление, документирование, реализация и поддержка процессов, процедур, а также мер для обеспечения требуемого уровня непрерывности информационной безопасности при неблагоприятных ситуациях.

7.2.12.3. Проверка установленных и реализованных мер по обеспечению непрерывности информационной безопасности, чтобы обеспечить уверенность в их актуальности и эффективности при возникновении неблагоприятных ситуаций.

7.2.12.4. Внедрение средств обработки информации с учетом резервирования, достаточного для выполнения требований доступности.

7.2.13. Соответствие

7.2.13.1. Определение законодательных, нормативных, контрактных требований, а также подхода ТИУ к удовлетворению этих требований, документирование и сохранение их актуальными для каждой информационной системы.

7.2.13.2. Защита записей от потери, уничтожения, фальсификации, несанкционированного доступа и разглашения в соответствии с правовыми, регулятивными, договорными и иными требованиями.

7.2.13.3. Обеспечение конфиденциальности и защиты персональных данных в соответствии с требованиями соответствующих законодательных и нормативных актов.

7.2.13.4. Использование криптографических мер обеспечения информационной безопасности с соблюдением требований всех соответствующих соглашений, правовых и регулятивных актов.

8. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящая политика вводится в действие с даты утверждения, регистрации в общем отделе и размещения в реестре нормативных документов и действует до отмены или принятия нового локального нормативного акта, регулирующего общие положения.

8.2. Внесение изменений и дополнений в настоящую политику осуществляется в установленном в ТИУ порядке.

8.3. Считать утратившим силу положение по информационной безопасности от 24.11.2016 №8ИТ-17/2016.