МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования **«Тюменский индустриальный университет»** Отдел информационной безопасности

УТВЕРЖДАЮ
И.о. ректора

_____Ю.С. Клочков
«_____» _____2024 г.

ПОЛОЖЕНИЕ
об отделе информационной безопасности

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее Положение регламентирует деятельность структурного подразделения федерального государственного бюджетного образовательного учреждения высшего образования «Тюменский индустриальный университет» (далее - ТИУ, Университет) – отдела информационной безопасности (далее - Отдел), основные цели, задачи, функции и организационную структуру Отдела и является его базовым нормативным документом.

1.2. Отдел осуществляет свою деятельность под руководством ректора Университета.

1.3. Возглавляет Отдел начальник, назначаемый на должность и освобождаемый от нее приказом ректора Университета.

1.4. На должность начальника Отдела назначается лицо, имеющее высшее образование (специалитет или магистратура) в области информационной безопасности и стаж работы в области информационной безопасности не менее 3 лет, или высшее образование (специалитет или магистратура) в области математических и естественных наук, инженерного дела, технологий и технических наук и стаж работы в области информационной безопасности не менее 5 лет, в том числе на руководящих должностях не менее 2 лет, или иное высшее образование (специалитет или магистратура) и стаж работы в области информационной безопасности не менее 5 лет, в том числе на руководящих должностях не менее 2 лет и прошедшего обучение по программам профессиональной переподготовки по одной из специальностей в области информационной безопасности (нормативный срок обучения - не менее 360 аудиторных часов).

1.5. Положение об Отделе, его структуру и штатное расписание утверждает ректор Университета.

1.6. Работники Отдела назначаются на должность и освобождаются от нее приказом ректора Университета по представлению начальника Отдела.

1.7. Ответственным за организацию документооборота Отдела является начальник.

2. ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ

2.1. Основные цели деятельности Отдела:

2.1.1. Исключение или существенное снижение негативных последствий (ущерба) в отношении Университета вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления в результате реализации угроз безопасности информации;

2.1.2. Обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

2.1.3. Противодействие техническим разведкам и техническая защита информации;

2.1.4. Повышение защищенности Университета от возможного нанесения ему материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем ТИУ или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования, а также иных внешних и внутренних действий любого характера;

2.1.5. Обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры Университета;

2.1.6. Обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры Университета.

2.2. Основные задачи Отдела:

2.2.1. Планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в Университете;

2.2.2. Выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств;

2.2.3. Предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;

2.2.4. Поддержание стабильной деятельности Университета и его производственных процессов в случае проведения компьютерных атак;

2.2.5. Взаимодействие с уполномоченными государственными органами и специализированными организациями по компьютерным инцидентам;

2.2.6. Обеспечение разработки локальных нормативным актов в сфере использования информационных ресурсов.

3. ФУНКЦИИ

3.1. Функции Отдела:

3.1.1. Разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в Университете;

3.1.2. Разработка локальных нормативных актов по обеспечению информационной безопасности в Университете;

3.1.3. Выявление и проведение анализа угроз безопасности информации в отношении Университета, уязвимостей информационных систем, программного обеспечения программно-аппаратных средств и принятие мер по их устранению;

3.1.4. Выявление попыток проникновения в состав персонала ТИУ источников криминальных структур, представителей иностранных спецслужб;

3.1.5. Предупреждение действий, наносящих ущерб информационным интересам ТИУ, со стороны отдельных лиц из числа работников ТИУ;

3.1.6. Обеспечение в соответствии с требованиями по информационной безопасности, в том числе с целью исключения (невозможности реализации) негативных последствий, разработки и реализации организационных мер и применения средств обеспечения информационной безопасности;

3.1.7. Установление обстоятельств разглашения информации ограниченного доступа;

3.1.8. Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

3.1.9. Представление в уполномоченные государственные органы и специализированные организации информации о выявленных компьютерных инцидентах;

3.1.10. Обеспечение проведения внутренних служебных расследований по фактам инцидентов, произошедших по линии информационной безопасности;

3.1.11. Исполнение указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих Университету либо используемых Университетом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

3.1.12. Осуществление взаимодействия с правоохранительными органами в предупреждении и пресечении правонарушений и преступлений в области информационной безопасности, направленных против законных интересов ТИУ и безопасности его работников и обучающихся;

3.1.13. Проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации) основных процессов Университета в целях обеспечения информационной безопасности в Университете;

3.1.14. Подготовка отчетов о состоянии работ по обеспечению информационной безопасности в Университете (Приложение);

3.1.15. Организация развития навыков безопасного поведения в Университете, в том числе проведение занятий с работниками Университета по вопросам обеспечения информационной безопасности;

3.1.16. Выполнение иных функций, исходя из поставленных ректором Университета целей и задач в рамках обеспечения информационной безопасности в ТИУ.

4. ПРАВА ОТДЕЛА

4.1. С целью реализации функций Отдел имеет право:

4.1.1. Добывать любыми разрешенными законодательством РФ способами информацию о совершенных и совершаемых в ущерб интересам Университета действиях в информационной сфере, а также о намерениях отдельных физических лиц совершить такие действия;

4.1.2. Использовать при осуществлении мероприятий по информационной безопасности технические, программные, программно-технические и иные средства, разрешенные законодательством РФ, не причиняющие вреда жизни и здоровью граждан и окружающей среде;

4.1.3. Беспрепятственно запрашивать в устной, либо иной форме и получать от работников Университета, независимо от должности, информацию и документы (по описи временной передачи документов), а также доступ к любым работам в структурных подразделениях Университета, необходимые для принятия решений по всем вопросам, отнесенным к компетенции Отдела, не раскрывая при этом целей запроса и доступа;

4.1.4. Беспрепятственно получать доступ и использовать имеющиеся в Университете информационные системы, базы данных, архивы и любые другие массивы документов;

4.1.5. Беспрепятственного перемещения на объекты (из объектов) Университета технических средств различного назначения, связанных с обеспечением информационной безопасности;

4.1.6. Беспрепятственного доступа в служебные помещения (комиссионно, с составлением акта осмотра – в нерабочее время, при отсутствии в помещении работников), осмотра территории Университета;

4.1.7. В случае необходимости привлекать работников структурных подразделений Университета к решению задач, связанных с обеспечением информационной безопасности Университета;

4.1.8. Готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности;

4.1.9. Контролировать деятельность любого структурного подразделения Университета по выполнению требований к обеспечению информационной безопасности, беспрепятственно осуществлять плановые и внеплановые проверки деятельности структурных подразделений ТИУ в области обеспечения информационной безопасности любыми, разрешенными законодательством, способами;

4.1.10. Повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности;

4.1.11. Участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ и организаций;

4.1.12. Участвовать в работе комиссий и советов Университета при рассмотрении вопросов и в целях обеспечения информационной безопасности;

4.1.13. Требовать в устной, либо иной форме от работников Университета незамедлительного прекращения работ или действий, создающих риски информационной безопасности Университета;

4.1.14. Вносить представления ректору Университета в отношении работников Университета при обнаружении фактов нарушения работниками установленных требований информационной безопасности в Университете, в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности;

4.1.15. Вносить на рассмотрение ректору Университета предложения по вопросам деятельности Отдела.

5. ПЕРЕЧЕНЬ ДОКУМЕНТОВ, ЗАПИСЕЙ И ДАННЫХ ПО ОСНОВНОЙ ДЕЯТЕЛЬНОСТИ ОТДЕЛА

5.1. Конституция РФ.

5.2. Гражданский кодекс Российской Федерации.

5.3. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».

5.4. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации».

5.5. Закон РФ от 21.07.1993 № 5485–I «О государственной тайне».

5.6. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

5.7. Федеральный закон от 29.12.2010 № 436-ФЗ «О защите детей от информации, причиняющей вред их здоровью и развитию».

5.8. Федеральный закон от 29.12.2012 № 273-ФЗ «Об образовании в Российской Федерации».

5.9. Постановление Правительства РФ от 15.07.2022 № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)».

5.10. Приказ Министерства связи и массовых коммуникаций РФ от 16.06.2014 № 161 «Об утверждении требований к административным и организационным мерам, техническим и программно-аппаратным средствам защиты детей от информации, причиняющей вред их здоровью и (или) развитию».

5.11. Приказ Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций от 14.11.2022 № 187 «Об утверждении Порядка и условий взаимодействия Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций с операторами в рамках ведения реестра учета инцидентов в области персональных данных».

5.12. Постановление Главного государственного санитарного врача РФ от 28.09.2020 № 28 «Об утверждении санитарных правил СП 2.4.3648-20 «Санитарно-эпидемиологические требования к организациям воспитания и обучения, отдыха и оздоровления детей и молодежи».

5.13. Устав ТИУ.

5.14. Коллективный договор ТИУ и Правила внутреннего трудового распорядка ТИУ.

5.15. Приказы и распоряжения руководства ТИУ, регламентирующие деятельность Отдела и его работников.

5.16. Номенклатура дел Отдела. Документы в соответствии с номенклатурой дел.

5.17. Положение об Отделе.

5.18. Должностные инструкции начальника и работников Отдела.

5.19. Штатное расписание Отдела.

5.20. Результаты внутренних и внешних аудитов СМК, проведенных в Отделе, и выполнение корректирующих действий, относительно деятельности Отдела и его работников.

5.21. Отчетные документы Отдела.

ВЗАИМООТОШЕНИЯ, СВЯЗИ, ОРГАНИЗАЦИОННАЯ СТРУКТУРА

6.1. Для выполнения функций и реализации прав Отдел взаимодействует с другими подразделениями ТИУ.

Наименование подразделения и/или должностные лица	Получение	Предоставление
Руководство ТИУ (Ректор, Ученый совет, Попечительский совет, Конференция работников и обучающихся)	– копии приказов, распоряжений, организационно - распорядительных документов по вопросам компетенции Отдела	– планы и отчеты о деятельности Отдела
Управление по работе с персоналом	– приказы по личному составу на согласование; – дополнительные соглашения к трудовым договорам на согласование; – приказы по командировкам; – выписки из протоколов по аттестации работников; – наградные документы работников; – согласованные должностные инструкции работников.	– графики отпусков работников Отдела; – заявления работников о предоставлении отпусков; – подписанные трудовые договоры; - документы по трудоустройству; - заявки на командировки работников; - заявки на повышение квалификации работников; - материалы для аттестации работников; - ходатайства о награждении работников; – проекты должностных инструкций работников; – и др. кадровые документы.
Финансово-экономическое управление	– выписок из штатного расписания по запросу; – информация по запросу	– служебных записок по формированию и изменению штатного расписания; – служебных записок на стимулирующие выплаты;
Отдел внутреннего аудита	– плана проведения аудиторских мероприятий; – программы внутреннего аудита СМК; – заключения по результатам проведения внутреннего аудита СМК	– план-отчета коррекции и корректирующих действий по результатам внутреннего аудита СМК; – прочих сведений
Иные	– по вопросам компетенции Отдела	– по вопросам компетенции Отдела

6.2. Отдел также взаимодействует с государственными и коммерческими структурами по вопросам, касающимся выполнения совместных работ.

ОРГАНИЗАЦИОННАЯ СТРУКТУРА ОТДЕЛА

7. ОТВЕТСТВЕННОСТЬ

7.1. Ответственность за организацию деятельности, качество выполнения возложенных настоящим Положением на Отдел задач, сохранность и целевое использование закрепленного имущества несет начальник Отдела.

7.2. Ответственность работников Отдела устанавливаются должностными инструкциями.

ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

8.1. Настоящее Положение вступает в силу после его утверждения, регистрации в общем отделе и размещения в реестре нормативных документов и действует до его отмены или принятия нового локального нормативного акта, регулирующего вопросы, указанные в п. 1.1 Положения.

8.2. Изменения и дополнения к настоящему Положению вносятся в установленном в Университете порядке.

8.3. Считать утратившим силу Положение об отделе информационной безопасности от 23.04.2024 № 12СП-290/2024.

Приложение

Документы и отчеты, подготавливаемые Отделом

Документ/отчет	Нормативная база, регулирующая составление	Сроки/ периодичность составления	Кому/ куда представляется
1	**2**	**3**	**4**
Отчет о состоянии обеспечения информационной безопасности	Письмо ФСТЭК России от 27.08.2024 № 2/752 дсп	до 01 февраля /Ежегодно	ФСТЭК России
Уведомление о фактах неправомерной или случайной передачи (предоставления, распространения, доступа) персональных данных, повлекшей нарушение прав субъектов персональных данных	Приказ Роскомнадзора от 14.11.2022 № 187	По мере возникновения	Роскомнадзор
Уведомление об инцидентах в области кибербезопасности	Письмо Минобрнауки России от 11.03.2022 № МН-19/275-АН	По мере возникновения	Минобрнауки России