МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Тульский государственный университет»

Утверждено
решением Ученого совета
протокол от 27.12.18 .№ 4
Ректор
_____ М. В. Грязев

ПОЛОЖЕНИЕ О СТРУКТУРНОМ ПОДРАЗДЕЛЕНИИ ТулГУ

ОТДЕЛ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ПСП ТулГУ ОИБ-2018

Проректор по ФД	А.А. Маликов
Начальник УИТиА	А.В Савельев
Начальник ОМКОД	Е.А. Саввина
Начальник ПЭУ	С.И. Триденская
Начальник ЮУ	Н.Я. Матвеева
Ученый секретарь	Л.И. Лосева
Председатель профкома работников ТулГУ	М.В. Лунев
Начальник ОИБ	А.В. Супонин

1 Общие положения

1.1 Настоящее положение регулирует деятельность Отдела информационной безопасности (ОИБ) – который является структурным подразделением Управления информационных технологий и автоматизации (далее УИТиА) Тульского государственного университета (далее университета).

1.2 ОИБ образовано в соответствии с приказом ректора университета от 02 августа 2007 года № 1160.

1.3 ОИБ административно подчиняется начальнику УИТиА.

1.4 ОИБ решает комплексные задачи по обеспечению и контролю информационной безопасности в университете.

1.5 Основными документами, регламентирующими деятельность отдела, являются:

- действующее законодательство и другие правовые нормативные акты РФ в области образования;
- приказы и инструктивные документы Министерства образования и науки РФ;
- устав ФГБОУ ВО Тульский государственный университет;
- политика в области качества и миссия ФГБОУ ВО ТулГУ;
- решения Учёного совета университета, приказы ректора и распоряжения проректоров;
- положение о защите информации;
- политика в отношении обработки персональных данных;
- правила обработки персональных данных;
- действующее законодательство в области защиты информации: Федеральный закон от 27 июля 2006 г. №152- ФЗ «О персональных данных», Федеральный закон от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации», Приказ Мининформсвязи РФ от 9 января 2008 г. №1 «Об утверждении требований по защите сетей связи от несанкционированного доступа к ним и передаваемой посредством их информации», Федеральный закон от 29 июля 2004 г. №98-ФЗ «О коммерческой тайне» и другие правовые нормативные акты РФ;
- рекомендации организаций, осуществляющих проверку деятельности университета;
- должностные инструкции работников отдела;
- правила внутреннего трудового распорядка.

1.6 ОИБ возглавляется начальником отдела, который назначается и освобождается от должности приказом ректора университета по представлению начальника Управления информационных технологий и автоматизации.

1.7 На должность начальника отдела, принимаются лица, отвечающие следующим квалификационным требованиям в соответствии с Профессиональным стандартом «06.032 Специалист по безопасности

компьютерных систем и сетей» регистрационный № 842, утвержденный приказом №598н от 01.11.2016:

- высшее образование (техническое);
- наличие опыта работы в области информационных технологий не менее 5 лет;
- наличие опыта работы руководителем проектов в области ИТ в течение двух лет;
- не менее пяти лет работы по применению и анализу эффективности средств защиты информации компьютерных систем, в том числе на руководящих должностях не менее трех лет;
- не менее трех лет работы по применению и анализу эффективности средств защиты информации компьютерных систем, в том числе на руководящих должностях не менее двух лет.

1.8 Создание, реорганизация и ликвидация отдела осуществляется в порядке, предусмотренном Уставом ТулГУ.

1.9 Функционирование ОИБ обеспечивается:

- обязательным участием всех работников отдела в организации и обеспечении его деятельности;
- исполнением всеми работниками отдела решений Ученого Совета университета, руководства университета и распоряжений начальника отдела.

1.10 Планирование деятельности ОИБ осуществляется на основании разработанных методик и мероприятий на календарный год.

1.11 Отчетность ОИБ включает в себя:

- письменный отчет о проделанной работе за прошедший год, ежегодно в первом квартале календарного года начальнику УИТиА;
- устный отчет, представляемый начальнику УИТиА в текущем порядке.

2 Функции

Функциями ОИБ являются:

2.1 Определение угроз безопасности и их возможных источников.

2.2 Определение каналов утечки информации.

2.3 Оценка эффективности реализуемых технических решений.

2.4 Оценка технико-экономического уровня реализуемых технических решений.

2.5 Выбор средств и методов защиты информации.

2.6 Разработка технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами.

2.7 Разработка рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации.

2.8 Определение потребности в средствах защиты информации, составление заявок на их приобретение с обоснованиями и расчетами.

2.9 Подготовка предложений по заключению соглашений и договоров с другими учреждениями, организациями, предоставляющими услуги в области защиты информации.

2.10 Выполнение аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации.

2.11 Выполнение контрольных проверок работоспособности и эффективности систем и средств защиты информации.

2.12 Анализ существующих методов и средств, применяемых для контроля и защиты информации.

2.13 Разработка предложений по совершенствованию и повышению эффективности методов и средств, применяемых для контроля и защиты информации.

2.14 Подготовка проектов нормативных и методических материалов, регламентирующих работу по защите информации.

2.15 Разработка организационно-распорядительных документов по защите информации.

2.16 Контроль над работой по оценке технико-экономического уровня разрабатываемых мер по защите информации.

2.17 Методическое руководство работой по оценке технико-экономического уровня разрабатываемых мер по защите информации.

2.18 Контроль над соблюдением установленного порядка выполнения работ, а также действующего законодательства Российской Федерации при решении вопросов, касающихся защиты информации.

2.19 Организация проведения специальных исследований и контрольных проверок по выявлению возможных каналов утечки информации.

2.20 Обеспечение соблюдения режима конфиденциальности проводимых работ.

2.21 Разработка регламента допуска работников университета к отдельным каналам информации, плана защиты информации, положений об определении степени защищенности ресурсов автоматизированных систем.

2.22 Соблюдение действующих инструкций по режиму работ и принятие своевременных мер по предупреждению нарушений.

2.23 Обеспечение соответствия проводимых работ технике безопасности, правилам и нормам охраны труда.

3 Основные задачи

3.1 Создание и развитие системы информационной безопасности университета, позволяющей в рамках закона организовывать работу университета.

3.2 Организация работ, связанных с защитой и сохранности информации, являющейся персональными данными или коммерческой тайной.

3.3 Оказание услуг по внедрению современных технологий связанных с зашитой информации.

4 Организационная структура

4.1 Состав и штатную численность отдела информационной безопасности утверждает ректор исходя из условий и особенностей деятельности по представлению начальника отдела и по согласованию с планово-экономическим Управлением.

4.2 В состав отдела входят инженеры информационной безопасности, отвечающие за отдельные направления в работе (за анализ состояния информационных баз, определение требований к защищенности различных подсистем автоматизированной системы университета и выбор методов и средств обеспечения их защиты, а также за разработку необходимых нормативно-методических и организационно-распорядительных документов по вопросам обеспечения информационной безопасности; за эффективное применение и администрирование штатных для операционных систем и систем управления базами данных и дополнительных специализированных средств защиты и анализа защищенности ресурсов автоматизированных систем).

5 Трудовые функции, трудовые действия, знания, умения начальника отдела

5.1 Трудовая функция - Разработка требований к программно-аппаратным средствам защиты информации компьютерных систем и сетей.

5.1.1 В целях реализации трудовой функции 5.1 начальник отдела обязан выполнять следующие трудовые действия:

- определение угроз безопасности и их возможных источников;
- определение каналов утечки информации;
- оценка эффективности реализуемых технических решений;
- оценка технико-экономического уровня реализуемых технических решений;
- выбор средств и методов защиты информации.

5.1.2 В целях реализации трудовой функции 5.1 начальник отдела должен уметь:

- обобщать научно-техническую литературу, нормативные и методические материалы в области защиты информации;
- формировать модели угроз и модели нарушителя безопасности компьютерных систем;
- выявлять наиболее целесообразные подходы к обеспечению защиты информации компьютерной системы;
- разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками;
- применять действующую законодательную базу в области обеспечения компьютерной безопасности;
- осуществлять принятие решений о необходимости использования

программно-аппаратных средств защиты информации.

5.1.3 В целях реализации трудовой функции 5.1 начальник отдела должен знать:

- порядок организации работ по защите информации;
- методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях;
- методы анализа безопасности компьютерных систем;
- методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных;
- принципы построения средств защиты информации компьютерных систем;
- нормативные правовые акты в области защиты информации;
- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- организационные меры по защите информации.

5.2 Трудовая функция - Проектирование программно-аппаратных средств защиты информации компьютерных систем и сетей.

5.2.3 В целях реализации трудовой функции 5.2 начальник отдела обязан выполнять следующие трудовые действия:

- разработка технических заданий, эскизных, технических и рабочих проектов работ по защите информации;
- разработка планов и графиков проведения работ по защите информации;
- анализ существующих методов и средств, применяемых для контроля и защиты информации;
- разработка предложения по совершенствованию существующих методов и средств, применяемых для контроля и защиты информации и повышению эффективности этой защиты;
- оценка технико-экономического уровня и эффективности предлагаемых и реализуемых технических решений;
- организация аттестации программ и алгоритмов на предмет соответствия требованиям защиты информации.

5.2.2 В целях реализации трудовой функции 5.2 начальник отдела должен уметь:

- проводить исследования с целью нахождения наиболее целесообразных практических решений по обеспечению защиты информации;
- подбирать и обобщать научно-техническую литературу, методические материалы по программным и аппаратным средствам и способам защиты информации, в том числе на английском языке.

5.2.3 В целях реализации трудовой функции 5.2 начальник отдела должен знать:

- методы и средства получения, обработки и передачи информации в операционных системах, системах управления базами данных и компьютерных сетях;
- виды атак и механизмы их реализации в компьютерных системах;
- методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных;
- принципы построения систем защиты информации компьютерных систем, в том числе антивирусного программного обеспечения;
- методы анализа безопасности компьютерных систем;
- нормативные правовые акты в области защиты информации.

5.3 Трудовая функция - Сопровождение средств защиты информации компьютерных систем и сетей.

5.3.1 В целях реализации трудовой функции 5.3 начальник отдела обязан выполнять следующие трудовые действия:

- разработка технических заданий, планов и графиков проведения работ по защите информации в соответствии с действующим нормативными и методическими документами;
- разработка рекомендаций и предложений по совершенствованию и повышению эффективности защиты информации;
- составление и оформление разделов технических отчетов;
- определение потребности в средствах защиты информации, составление заявок на их приобретение с необходимыми обоснованиями и расчетами;
- подготовка предложений по заключению соглашений и договоров с другими учреждениями, организациями, предоставляющими услуги в области защиты информации;
- выполнение контрольных проверок работоспособности и эффективности систем и средств защиты информации;
- анализ существующих методов и средств, применяемых для контроля и защиты информации;
- разработка предложений по совершенствованию и повышению эффективности методов и средств, применяемых для контроля и защиты информации;
- подготовка проектов нормативных и методических материалов, регламентирующих работу по защите информации;
- разработка организационно-распорядительных документов по защите информации.

5.3.2 В целях реализации трудовой функции 5.3 начальник отдела должен уметь:

- формировать модели угроз и модели нарушителя безопасности компьютерных систем;
- разрабатывать частные политики безопасности компьютерных систем, в том числе политики управления доступом и информационными потоками;
- применять действующую законодательную базу в области обеспечения защиты информации.

5.3.3 В целях реализации трудовой функции 5.3 начальник отдела должен знать:

- методы и средства получения, обработки и передачи информации;
- методы выявления каналов утечки информации;
- методы и средства защиты информации в компьютерных сетях, операционных системах и системах управления базами данных;
- методы анализа безопасности компьютерных систем;
- виды атак и механизмы их реализации в компьютерных системах;
- принципы построения систем защиты информации компьютерных систем;
- руководящие и методические документы уполномоченных федеральных органов исполнительной власти по защите информации;
- организационные меры по защите информации.

5.4 Трудовая функция – Организационное и методологическое обеспечение согласования документации.

5.4.1 В целях реализации трудовой функции 5.4 начальник отдела обязан выполнять следующие трудовые действия:

- назначение ответственных за согласование и утверждение документов;
- контроль исполнения.

5.4.2 В целях реализации трудовой функции 5.4 начальник отдела должен знать: .

- инструменты и методы выдачи и контроля поручений;
- инструменты и методы коммуникаций;
- каналы коммуникаций;
- модели коммуникаций;
- методы проведения рабочих и формальных согласований документации.

5.4.3 В целях реализации трудовой функции 5.4 начальник отдела должен уметь:

- разрабатывать планы и регламентные документы;
- контролировать исполнение регламентных документов.

5.5 Трудовая функция – Планирование управления персоналом в области ИТ.

5.5.1 В целях реализации трудовой функции 5.5 начальник отдела обязан выполнять следующие трудовые действия:

- определение потребности проекта в персонале с учетом квалификационных требований;
- разработка системы мотивации персонала в проекте.

5.5.2 В целях реализации трудовой функции 5.5 начальник отдела должен знать:

- управление персоналом в проектах;
- мотивация персонала;
- технологии межличностной и групповой коммуникации в деловом взаимодействии.

5.5.3 В целях реализации трудовой функции 5.5 начальник отдела должен уметь:

- планировать работы в проекте;
- проводить переговоры.

6 Права и обязанности начальника ОИБ

6.1 Права начальника ОИБ:

- руководить (путем отдачи распоряжений и поручений) работниками ОИБ, а также получать отчеты в устной форме о выполненной работе:
- подбирать кадры для ОИБ;
- визировать документы ОИБ в пределах своей компетенции и документы других подразделений в рамках выполнения своих функциональных обязанностей;
- осуществлять контроль над деятельностью структурных подразделений университета по выполнению ими требований информационной безопасности;
- давать структурным подразделениям университета и отдельным специалистам обязательные для исполнения указания по вопросам, входящим в компетенцию отдела;
- запрашивать и получать от структурных подразделений сведения, справочные и другие материалы, необходимые для осуществления деятельности отдела;
- вести самостоятельную переписку с государственными и муниципальными органами по правовым вопросам;
- представлять в установленном порядке университет в органах государственной власти, иных учреждениях и организациях, по вопросам, входящим в компетенцию отдела;
- обязан принимать меры при обнаружении несанкционированного доступа к информации как внутри университета, так и извне и докладывать о принятых мерах руководителю университета с представлением информации о субъектах, нарушивших режим доступа;
- по согласованию с начальником УИТиА или проректором по финансовой деятельности привлекать экспертов и специалистов в сфере защиты

информации для консультаций, подготовки заключений, рекомендаций и предложений.

6.2 Обязанности начальника ОИБ:

- выполнять трудовые функции, трудовые действия, обладать необходимыми знаниями и умениями, перечисленными в разделе 5;
- разрабатывать проекты текущих и перспективных планов совершенствования информационной защиты университета;
- составлять текущие и перспективные планы работы отдела;
- планировать и распределять работу в отделе;
- контролировать своевременное и качественное выполнение всех работ, обеспечивать условия для выполнения этих работ;
- своевременно представлять отчеты о работе ОИБ, планы перспективных мероприятий, ответы на обращения к отделу;
- принимать участие в разработках пакетов прикладных программ, систем и технических проектов, выполняемых по планам отдела;
- проводить производственные собрания, совещания;
- осуществлять контроль над соблюдением инструкций по технике безопасности и противопожарной безопасности;
- выполнять правила внутреннего трудового распорядка;
- повышать свою квалификацию.

7 Ответственность

7.1 Начальник ОИБ несет ответственность за:

- ненадлежащее и несвоевременное выполнение функций отдела;
- необеспечение сохранности принятых на ответственное хранение программных и технических средств;
- необеспечение сохранности принимаемой информации и достоверности передаваемой;
- несвоевременное, а также некачественное исполнение документов и поручений руководства университета и внешней нормативной документации;
- допущение использования информации работниками отдела в неслужебных целях;
- ненадлежащий контроль над режимом доступа к информации, повлекшего утечку информации, повреждение информационных баз данных;
- ненадлежащее ведение внешней нормативной документации.

8 Номенклатура дел ОИБ

Номенклатура дел отдела информационной безопасности представлена в таблице 1.

Таблица 1 – Номенклатура дел отдела

Индекс дела	Заголовок дела (тома, части)	Кол-во дел (томов, частей)	Срок хранения и № статей по перечню	Примечание
1	2	3	4	5
4-04-01	**Отдел информационной безопасности**			
4-04-01-01	Годовые планы работ ОИБ		5л. ст.290	
4-04-01-02	Приказы, распоряжения ректора (проректоров) ТулГУ (копии)		ДМН	Подлинники в общем отделе и СЭД «Дело»
4-04-01-03	Информационно-справочные документы, памятки		ДМН ст.535 б	
4-04-01-04	Протоколы заседаний ОИБ		Пост. ст.18 б	
4-04-01-05	Журналы учета входящих и исходящих документов		5л. ст.258 г	
4-04-01-06	Годовые отчеты ОИБ		5л. ст.475	
4-04-01-07	Положение об ОИБ (копия)		ДМН	Подлинник в ПФО
4-04-01-08	Должностные инструкции работников ОИБ (копия)		ДМН	Подлинник в ПФО
4-04-01-09	Инструкции по технике безопасности (копии)		ДМН	Подлинник в УБЖ
4-04-01-10	Журнал регистрации нештатных ситуаций		5 л. ст.230	
4-04-01-11	Переписка с организациями по вопросам работы отдела (входящая)		5л. ЭПК ст.35	
4-04-01-12	Переписка с организациями по вопросам работы отдела (исходящая)		5л. ЭПК ст.35	
4-04-01-13	Положение о защите информации		3г. ст.219 б	ПЗН
4-04-01-14	Журнал регистрации и выдачи ключевых носителей		5л. ст.260 г, 260 е	После замены ключа
4-04-01-16	Сертификаты ключей ЭЦП		Пост. ст.232	
4-04-01-17	Лицензии, сертификаты соответствия		Пост. ст.97	
4-04-01-20	Документы стратегического развития ТулГУ (стандарты системы менеджмента качества, Политика в области качества, Миссия ТулГУ) (действующие) (копии)		ДМН	Подлинники в ОМКОД В электронном виде http://tsu.tula.ru/
4-04-01-21	Номенклатура дел отдела		ДЗН ст.200 б	

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Номер изменения	Номер листа				Всего листов в документе	Дата внесения изменения	Дата введения изменения в действие	Подпись лица, ответственного за внесение изменений
	измененного	замененного	нового	изъятого				