МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В.Н. Татищева»
(Астраханский государственный университет им. В.Н. Татищева)

УТВЕРЖДАЮ

Ректор

_____ И.А. Алексеев

«_05_» _____мая_____ 2025 г.

ПОЛОЖЕНИЕ
об отделе информационной безопасности ФГБОУ ВО «Астраханский государственный университет им. В.Н. Татищева»

Астрахань – 2025

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Настоящее типовое положение определяет цели, задачи и функции отдела информационной безопасности ФГБОУ ВО «Астраханский государственный университет имени В.Н. Татищева» (далее – Университет).

1.2. Отдел информационной безопасности (далее – Отдел) является структурным подразделением управления информационных технологий и систем.

1.3. Отдел создается, реорганизуется и ликвидируется приказом ректора Университета.

1.4. Деятельность Отдела курирует начальник управления информационных технологий и систем.

1.5. Непосредственное руководство Отдела осуществляет начальник отдела информационной безопасности, назначаемый и освобождаемый от занимаемой должности приказом ректора Университета.

1.6. Отдел в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и актами Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, другими нормативными правовыми документами в сфере обеспечения информационной безопасности, приказами ректора Университета.

2. СТРУКТУРА ОТДЕЛА

2.1. Численность сотрудников Отдела определяется текущими задачами, функционалом подразделения и штатным расписанием.

2.2. Начальник Отдела распределяет обязанности между сотрудниками и составляет их должностные инструкции по согласованию с начальником управления информационных технологий и систем.

2.3. Работники Отдела назначаются и освобождаются от должности в порядке, предусмотренном трудовым законодательством Российской Федерации.

3. ОСНОВНЫЕ ЦЕЛИ И ЗАДАЧИ

3.1. Деятельность отдела информационной безопасности направлена на достижение следующих целей:

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

– обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;

– повышение защищенности информационной инфраструктуры Университета от возможного нанесения ему материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных ресурсов Университета или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;

– обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры Университета;

– обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных ресурсов и информационно-телекоммуникационной инфраструктуры Университета.

3.2. Основными задачами деятельности подразделения являются:

– планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в Университете;

– выявление угроз безопасности информации и уязвимостей информационных ресурсов, программного обеспечения и программно-аппаратных средств;

– 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;

– поддержание стабильной деятельности Университета и его производственных процессов в случае проведения компьютерных атак;

– взаимодействие с Национальным координационным центром по компьютерным инцидентам;

– обеспечение нормативно-правового обеспечения использования информационных ресурсов.

4. ОСНОВНЫЕ ФУНКЦИИ

Отдел выполняет следующие функции:

– Разработка концепции и политики информационной безопасности Университета, включая разработку регламентов, стандартов, руководств и должностных инструкций по информационной безопасности.

– Разработка организационно-распорядительной документации по информационной безопасности и доведение ее до сотрудников в части их касающейся.

– Разработка, координация, управление и контроль за реализацией плана работ по обеспечению информационной безопасности в Университете.

– Разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в Университете и представление их начальнику управления информационных технологий и систем.

– Выявление и проведение анализа угроз безопасности информации в отношении информационной инфраструктуры Университета, уязвимостей информационных ресурсов, программного обеспечения программно-аппаратных средств и принятие мер по их устранению.

– 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.

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

– Представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах.

– 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 либо используемых Университетом, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет».

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

– Организация и проведение плановых проверок режима защиты информации, разработка соответствующей документации, анализ результатов, расследование нарушений.

– Подготовка отчетов о состоянии работ по обеспечению информационной безопасности в Университете.

– Организация развития навыков безопасного поведения в Университете, в том числе проведение занятий с руководителями структурных подразделений, административным персоналом и профессорско-преподавательским составом Университета по вопросам обеспечения информационной безопасности.

– Обеспечение сотрудников университета информационной поддержкой по вопросам информационной безопасности.

– Выполнение иных функций, исходя из поставленных начальником управления информационных технологий и систем целей и задач в рамках обеспечения информационной безопасности в Университете.

– Формирование ключевых данных для входа пользователей в информационные ресурсы Университета.

– Формирование групповых политик доступа и ролей пользователей информационных ресурсов Университета.

5. ПРАВА И ОБЯЗАННОСТИ

С целью реализации функций отдел информационной безопасности имеет право:

– Запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений Университета, необходимым для принятия решений по всем вопросам, отнесенным к компетенции подразделения;

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

– Контролировать деятельность любого структурного подразделения Университета по выполнению требований к обеспечению информационной безопасности;

– Постоянно повышать профессиональные компетенции, знания и навыки работников отдела информационной безопасности и, назначенных ректором Университета, администраторов информационной безопасности;

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

– Участвовать в работе комиссий Университета при рассмотрении вопросов обеспечения информационной безопасности;

– Вносить предложения руководству Университета о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;

– Вносить представления руководству Университета в отношении руководителей структурных подразделений, административного персонала и профессорско-преподавательского состава Университета при обнаружении фактов нарушения работниками установленных требований безопасности информации в Университета, в том числе ходатайствовать о привлечении указанных работников к административной или уголовной ответственности;

– Вносить на рассмотрение начальника управления информационных технологий и систем Университета предложения по вопросам деятельности отдела информационной безопасности.

На Отдел возлагается обязанность за:

– Организацию деятельности и осуществление контроля отдела по выполнению задач и функций, возложенных на отдел.

– Организацию в отделе оперативных и качественных подготовки и исполнения документов, ведения делопроизводства в соответствии с действующими правилами и инструкциями.

– Осуществление контроля за соблюдением работниками отдела трудовой и производственной дисциплины.

– Обеспечение сохранности имущества, закрепленного за отделом, и соблюдение правил пожарной безопасности.

– Соответствие законодательству разработанных отделом проектов приказов, инструкций, положений и других документов.

6. ОТВЕТСТВЕННОСТЬ

6.1 Ответственность за ненадлежащее и несвоевременное выполнение отделом функций, предусмотренных настоящим Положением, несет начальник отдела.

6.2 Ответственность за неисполнение обязанностей Отдела, указанных в настоящем Положении, несет начальник отдела.

6.3 Ответственность работников отдела устанавливается должностными инструкциями.

Сотрудники отдела информационной безопасности несут ответственность за:

– невыполнение должностных инструкций;

– не соблюдение требований настоящего Положения и Устава АГУ им. В.Н. Татищева, внутренних правил и инструкций, в том числе правил техники безопасности и противопожарной безопасности;

– не сохранность доверенных им материальных ценностей.

7. ВЗАИМООТНОШЕНИЯ И СВЯЗИ ПОДРАЗДЕЛЕНИЯ

7.1 Отдел информационной безопасности осуществляет свои полномочия во взаимодействии со структурными подразделениями Университета.

7.2 По указанию ректора, начальника управления информационных технологий и систем Университета осуществляется взаимодействие с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю, Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации по вопросам информационной безопасности, Министерством науки и высшего образования Российской Федерации.

-пятидневная рабочая неделя с выходными днями суббота и воскресенье;

-начало рабочего дня: 9 часов 00 минут по местному времени;

-окончание рабочего дня: 17 часов 30 минут по местному времени;

-перерыв для отдыха и питания с 12 часов 30 минут до 13 часов 00 минут по местному времени.

7.6. Обязанности, права и ответственность, а также оплата труда работников Отдела определяются Правилами внутреннего трудового распорядка, должностными инструкциями, трудовыми договорами, штатным расписанием и иными локальными нормативными актами Университета.

Начальник отдела: В.А. Корякова

СОГЛАСОВАНО:

Проректор по образовательной деятельности и цифровизации Г.В. Станкевич

Начальник управления информационных технологий и систем Д.Э. Шукралиева

Начальник управления по работе с персоналом И.А. Говорунова

И.о. начальника управления правового и организационного обеспечения Д.В. Ковалев