

Утверждено приказом
от « 11 » ноября 2021 г. № 2369-0

ПОЛОЖЕНИЕ
об отделе информационной безопасности
департамента информационных технологий

Ставрополь, 2021

1. Общие положения

1.1. Настоящее Положение определяет правовой статус, функции и полномочия (регламентирует организацию работы, права, обязанности), ответственность отдела информационной безопасности департамента информационных технологий федерального государственного автономного образовательного учреждения высшего образования «Северо-Кавказский федеральный университет» (далее – ОИБ, СКФУ), а также порядок его взаимодействия с другими структурными подразделениями СКФУ.

1.2. ОИБ является структурным подразделением СКФУ, входящим в состав департамента информационных технологий (далее – ДИТ) и специализируется на планировании, организации и обеспечении выполнения мероприятий, связанных с проектированием, внедрением и эксплуатацией средств и технологий безопасности информации, передаваемой и обрабатываемой в информационных сетях, системах и центрах обработки данных СКФУ.

1.3. ОИБ в своей деятельности руководствуется Конституцией Российской Федерации, действующими нормативными правовыми актами Российской Федерации, уставом СКФУ, решениями Ученого совета СКФУ, приказами и распоряжениями ректора СКФУ, Правилами внутреннего трудового распорядка СКФУ, Положением о ДИТ, настоящим Положением и иными локальными нормативными актами СКФУ.

1.4. ОИБ находится в непосредственном подчинении директора департамента информационных технологий (далее – директор ДИТ).

1.5. Структуру, численность и штатное расписание, изменения в структуру и штатное расписание ОИБ утверждает ректор СКФУ.

1.6. ОИБ возглавляет начальник отдела информационной безопасности (далее – начальник ОИБ), принимаемый на работу и освобождаемый от должности приказом СКФУ.

1.7. Условия труда работников ОИБ определяются трудовыми договорами, заключаемыми с каждым работником, а также Правилами внутреннего трудового распорядка СКФУ.

1.8. Права, обязанности, степень ответственности работников ОИБ устанавливаются должностными инструкциями.

1.9. Положение об ОИБ, вносимые в него изменения утверждаются приказом СКФУ.

2. Цели и задачи

2.1. Основными целями ОИБ являются создание технических и организационных условий безопасного функционирования объектов информационно-телекоммуникационной инфраструктуры и автоматизированных информационных систем университета, координация деятельности структурных подразделений университета для обеспечения защиты информации при ее автоматизированной обработке.

2.2. Основными задачами ОИБ являются обеспечение выполнения требований действующего законодательства Российской Федерации, иных нормативных и правовых актов по защите информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, в том числе персональных

данных, передаваемой и обрабатываемой в информационных сетях, системах и центрах обработки данных СКФУ, (далее – информация с ограниченным доступом).

3. Функции

3.1. Организация мероприятий по определению, утверждению, актуализации и ведению перечней категорий информации с ограниченным доступом, обрабатываемой в информационных сетях и автоматизированных системах университета, и подлежащей защите в соответствии с действующими требованиями федерального законодательства, нормативных и руководящих документов.

3.2. Организация мероприятий по определению, утверждению, актуализации и ведению перечней лиц, допущенных к обработке категорий информации с ограниченным доступом в информационных сетях и автоматизированных системах университета.

3.3. Организация мероприятий по определению, утверждению, актуализации и ведению перечней информационных ресурсов и систем университета, в том числе информационных систем персональных данных, обрабатывающих информацию с ограниченным доступом и подлежащих защите.

3.4. Организация и контроль за выполнением мероприятий по защите информации с ограниченным доступом, обрабатываемой в информационных сетях и автоматизированных системах университета, в том числе во вновь создаваемых и модернизируемых.

3.5. Актуализация моделей угроз и нарушителей, матриц угроз и рисков, иных ключевых элементов формирования и исполнения политики информационной безопасности, разработка частных моделей и схем оценки информационной безопасности, необходимых для постоянной адаптации систем защиты информации к изменяющимся условиям.

3.6. Разработка технических заданий на проведение работ, оказание услуг, поставку, внедрение и сопровождение средств, систем и технологий, направленных на совершенствование защиты информации с ограниченным доступом, проведение приемо-сдаточных испытаний и приемка результатов работ.

3.7. Организация и проведение работ по определению состава, внедрению и обеспечению функционирования средств криптографической защиты информации и электронной подписи, средств защиты информации от несанкционированного доступа и иных средств, необходимых для защиты информации с ограниченным доступом, в соответствии с требованиями действующего законодательства, нормативных и руководящих документов.

3.8. Разработка и согласование спецификаций и состава программных и аппаратных средств защиты информации, приобретаемых университетом, участие в подготовке разделов по направлениям деятельности ОИБ в комплексных проектах, разрабатываемых по другим направлениям деятельности.

3.9. Организация администрирования информационной безопасности информационно-коммуникационных систем, систем обработки и хранения данных и автоматизированных информационных систем университета в процессе их проектирования, внедрения и эксплуатации.

3.10. Организация и контроль проведения мероприятий по оценке эффективности принимаемых мер по обеспечению безопасности информации.

3.11. Обеспечение применения сертифицированных по требованиям безопасности информации средств защиты информации во всех необходимых случаях.

3.12. Организация и обеспечение ведения учета применяемых в университете средств защиты информации, носителей ключевой информации и иных специализированных средств по направлениям деятельности ОИБ.

3.13. Осуществление комплекса мероприятий по развитию и функционированию инфраструктуры открытых и закрытых ключей, в т.ч. по обеспечению работы удостоверяющего центра и/или по взаимодействию с внешними удостоверяющими центрами, по обеспечению функционирования средств юридически значимого электронного документооборота.

3.14. Участие в установленном порядке в расследовании причин и условий появления нарушений в области информационной безопасности, разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

3.15. Анализ причин и последствий возможных и произошедших нарушений информационной безопасности, разработка предложений по организации и совершенствованию системы защиты информации.

3.16. Оказание методической помощи структурным подразделениям университета в выполнении организационных и технических мероприятий по защите информации, организация контроля за их выполнением.

3.15. Указанные функции при необходимости выполняются совместно с Управлением комплексной безопасности (далее - УКБ) в соответствии с утверждённым в СКФУ порядком разделения зон ответственности и организации взаимодействия.

4. Права и обязанности

4.1. Работники ОИБ имеют право:

- истребовать от подразделений СКФУ (по согласованию с директором департамента) информацию и документы, необходимые для осуществления деятельности ОИБ;

- привлекать с согласия руководителей структурных подразделений СКФУ работников этих подразделений для участия в подготовке проектов локальных актов и других документов, а также для участия в разработке и осуществлении мероприятий, проводимых ОИБ;

- участвовать в проводимых руководством университета совещаниях при обсуждении на них вопросов, имеющих непосредственное отношение к деятельности ОИБ;

- вносить директору ДИТ предложения об отмене, внесении изменений и дополнений в локальные акты СКФУ;

- осуществлять взаимодействие с подразделениями СКФУ, органами государственной власти, судебными и надзорными органами, юридическими и физическими лицами по вопросам, отнесенным к компетенции ОИБ.

4.2. Работники ОИБ обязаны:

- соблюдать устав СКФУ, Правила внутреннего трудового распорядка СКФУ, правила охраны труда и техники безопасности, правила пожарной безопасности;

- выполнять требования приказов, распоряжений и поручений руководства СКФУ и ДИТ;
- выполнять возложенные на них функции;
- совершенствовать и развивать деятельность СКФУ, обеспечиваемую ОИБ;
- давать разъяснения по вопросам, относящимся к компетенции ОИБ;
- совершенствовать свою деятельность как при помощи материально-технических средств, так и путем повышения уровня квалификации и ответственности каждого работника ОИБ;
- сохранять конфиденциальность сведений, содержащихся в документах, поступающих в ОИБ и/или подготавливаемых им.

4.3. Начальник ОИБ имеет право:

- запрашивать (по согласованию с директором ДИТ) у руководителей других структурных подразделений СКФУ информацию и документы, необходимые для выполнения задач и функций, возложенных на ОИБ;
- принимать участие в проводимых руководством совещаниях при обсуждении на них вопросов, имеющих непосредственное отношение к работе ОИБ;
- требовать соблюдения работниками ОИБ устава СКФУ, Правил внутреннего трудового распорядка СКФУ, правил охраны труда и техники безопасности, правил противопожарной безопасности, выполнения приказов, распоряжений и поручений руководства СКФУ.

4.4. Начальник ОИБ обязан:

- руководить работой ОИБ, обеспечивать выполнение задач и функций, определенных настоящим Положением, а также приказов, распоряжений и поручений руководства СКФУ;
- вносить (по согласованию с директором ДИТ) предложения ректору СКФУ о совершенствовании деятельности ОИБ и повышении эффективности его работы;
- руководить разработкой проектов нормативно-методических документов, связанных с организацией деятельности ОИБ;
- вносить предложения по подбору кадров в ОИБ, по проведению профессиональной подготовки (переподготовки) и повышения квалификации работников ОИБ, контролировать и обеспечивать знание работниками актуального состояния нормативных требований в области защиты информации, инструментальных средств и технологий защиты информации;
- подготавливать проекты должностных инструкций работников ОИБ, согласовывать их с директором ДИТ;
- вносить ректору СКФУ представления о поощрении работников ОИБ и применении к ним дисциплинарных взысканий;
- обеспечивать создание на рабочих местах оптимальных условий для высокопроизводительного и качественного труда;
- контролировать соблюдение работниками ОИБ Правил внутреннего трудового распорядка СКФУ, правил охраны труда и техники безопасности, правил противопожарной безопасности;
- участвовать в разработке и осуществлении мер по обеспечению сохранности имущества СКФУ.

4.5. Иные права и обязанности начальника ОИБ определяются должностной инструкцией и трудовым договором.

5. Ответственность

5.1. Работники ОИБ в пределах, определённых действующим трудовым законодательством, несут персональную ответственность за:

5.1.1. Несоблюдение законодательства Российской Федерации, достоверность информации, представляемой ОИБ руководству СКФУ;

5.1.2. Ненадлежащее исполнение или неисполнение своих должностных обязанностей, предусмотренных должностной инструкцией.

5.1.3. Разглашение персональных данных сотрудников и обучающихся СКФУ, ставших известными работникам ОИБ в связи с исполнением должностных обязанностей;

5.1.4. Нарушение Правил внутреннего трудового распорядка СКФУ, правил противопожарной безопасности и техники безопасности, установленных в СКФУ;

5.1.5. Причинение вреда имуществу СКФУ в пределах, установленных действующим гражданским законодательством.

5.2. Всю полноту ответственности за качество и своевременное выполнение возложенных настоящим Положением на ОИБ задач и функций несет начальник ОИБ.

5.3. Степень ответственности работников ОИБ определяется их должностными инструкциями.

6. Прекращение деятельности отдела

6.1. Прекращение деятельности ОИБ производится приказом СКФУ.