Приложение
к приказу
от _____ № _____

Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И. о. ректора
_____ М.В. Румянцев
«____» _____ 2026 г.

ПОЛОЖЕНИЕ
о защите информации
ПВД ЗИ – 2026

Красноярск 2026

Содержание

1 Общие положения

1.1 Положение о защите информации Федерального государственного автономного образовательного учреждения высшего образования «Сибирский федеральный университет» (далее – Положение о защите информации СФУ, Положение) определяет:

– политику защиты информации Федерального государственного автономного образовательного учреждения высшего образования «Сибирский федеральный университет» (далее – Сибирский федеральный университет, СФУ, университет);

– цели, задачи, направления защиты информации, объекты, подлежащие защите;

– порядок организации защиты информации в университете;

– порядок допуска работников и обучающихся университета к работе с конфиденциальной информацией;

– порядок передачи (предоставление, распространение, доступ) конфиденциальной информации в другие организации и физическим лицам;

– порядок работы с конфиденциальной информацией;

– порядок организации защиты информации в информационных системах и сервисах;

– управление рисками информационной безопасности, реагирование на инциденты и угрозы информационной безопасности;

– организация и порядок проведения внутреннего контроля за состоянием защиты информации;

– другие аспекты защиты информации в университете.

1.2 Положение определяет порядок организации мероприятий по защите конфиденциальной информации и открытой (общедоступной) информации.

1.3 Требования Положения не распространяются на мероприятия по защите информации, составляющей государственную тайну.

1.4 В положении используются нижеследующие термины и определения:

– **автоматизированная система (АС):** система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций;

– **автоматизированное рабочее место (АРМ):** программно-технический комплекс, предназначенный для автоматизации деятельности определенного вида;

– **аутентификация:** проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности;

– **вредоносная программа:** программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы;

– **доступ к информации**: получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

– **доступность (санкционированная доступность) информации:** состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия;

– **защита информации (ЗИ):** деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

– **защищаемое помещение (ЗП):** помещение, в котором хранится, обрабатывается и циркулирует конфиденциальная информация, размещаются технические средства её хранения, обработки и передачи, другое важное техническое и телекоммуникационное оборудование. К числу защищаемых помещений могут быть отнесены также помещения, в которых хранится и обрабатывается открытая ценная (важная) информация;

– **идентификация:** процедура, в результате выполнения которой для субъекта идентификации выявляется его идентификатор, однозначно идентифицирующий этого субъекта в информационной системе. Для выполнения процедуры идентификации в информационной системе субъекту предварительно должен быть назначен соответствующий идентификатор (т.е. проведена регистрация субъекта в информационной системе);

– **информационная безопасность (безопасность информации):** состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность, целостность и доступность информации;

– **информационная система (ИС):** организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы;

– **информационная среда университета:** среда, обеспечивающая деятельность университета за счет использования информационных технологий; объединяет сетевые, вычислительные и информационные ресурсы, созданные и используемые в деятельности университета, и служит основой применения в университете передовых информационных технологий в управлении университетом, в учебном, научном и других процессах;

– **информационная технология:** приемы, способы и методы применения средств вычислительной техники при выполнении функций сбора, хранения, обработки, передачи и использования данных;

– **информационные ресурсы:** отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах);

– **инцидент информационной безопасности (инцидент ИБ):** одно или серия нежелательных или неожиданных событий в системе информационной безопасности, которые имеют большую возможность скомпрометировать деловые операции и поставить под угрозу защиту информации;

– **контролируемая зона (КЗ):** пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств;

– **конфиденциальная информация университета (КИ):** информация (персональные данные, коммерческая, служебная и другие предусмотренные законодательством виды тайн), не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации и в случаях служебной необходимости;

– **конфиденциальность информации:** сохранение информации в тайне от субъектов, не имеющих полномочий на ознакомление с ней;

– **машинные носители информации:** жесткие диски, внешние накопители на жестких дисках, флэш-накопители, компакт-диски, иные устройства, фото-, кино-, видео- и аудиопленки и др.;

– **мобильные электронные устройства:** устройства, типа ноутбук, блокнотный, планшетный и портативный компьютер, личный цифровой помощник (персональный цифровой секретарь), радиоприемник и радиопередатчик, средства аудио, фото, видеозаписи, средства мобильной связи и других устройств;

– **несанкционированный доступ/несанкционированные действия (НСД):** доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

– **несанкционированное воздействие на информацию:** воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке,

уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

– **объект информатизации (ОИ):** совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров;

– **открытая (общедоступная, ценная, важная) информация:** служебная и иная информация, учебные, учебно-методические и другие материалы, программное обеспечение, не относящиеся к сведениям конфиденциального характера, но нарушение целостности которых, их блокирование или утрата могут привести к нарушениям технологии обработки информации, принятию неправильных решений, ухудшению качества и оперативности производственного (учебного) процесса, реализации других угроз безопасности;

– **передача информации:** предоставление, распространение информации, доступ к информации;

– **предоставление информации:** действия, направленные на раскрытие информации определенному лицу или определенному кругу лиц;

– **распространение информации:** действия, направленные на раскрытие информации неопределенному кругу лиц;

– **риск информационной безопасности:** сочетание вероятности инцидента информационной безопасности и его последствий;

– **система защиты информации (СЗИ):** совокупность органов и (или) исполнителей, используемых ими средств, методов и мероприятий, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

– **событие безопасности (информационной):** идентифицированное возникновение состояния информационной системы (сегмента, компонента информационной системы), сервиса или сети, указывающее на возможное нарушение безопасности информации, или сбой средств защиты информации, или ранее неизвестную ситуацию, которая может быть значимой для безопасности информации.

– **угроза безопасности информации:** возможные действия или условия, приводящие к нарушению конфиденциальности, целостности и доступности информации преднамеренного или непреднамеренного характера;

– **управление рисками информационной безопасности:** процесс принятия и выполнения управленческих решений, направленных на снижение вероятности инцидентов информационной безопасности и минимизацию возможных потерь, вызванных их реализацией;

– **целостность информации:** устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

2 Политика защиты информации СФУ

2.1 Цель защиты информации обеспечение:

– информационной безопасности университета;

– устойчивой работы информационной среды университета;

– сбалансированных интересов (прав) работников, обучающихся и других граждан, университета и государства в информационной среде университета.

2.2 Объектами, подлежащими защите, являются:

– информационные ресурсы: конфиденциальная и общедоступная (открытая важная, ценная) информация на бумажных и машинных носителях информации, а также речевая информация;

– технические средства обработки и передачи информации: средства вычислительной техники (СВТ), автоматизированные системы (АС), информационные системы (ИС), сервисы, вычислительные сети (ВС), аппаратное и программное обеспечение этих систем, линии и средства связи, посредством которых передается конфиденциальная и другая информация, другие средства обработки и передачи информации;

– защищаемые помещения, а также помещения и объекты, в которых ведется хранение и обработка открытой общедоступной информации.

2.3 Защита информации представляет собой принятие правовых, организационных и технических мер, направленных на выполнение следующих задач:

– обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации;

– соблюдение конфиденциальности информации ограниченного доступа;

– реализацию права на доступ к информации.

2.4 Требования по защите общедоступной информации могут устанавливаться только для достижения целей, указанных в первом и третьем подпунктах пункта 2.3.

2.5 Университет, как оператор информационных систем в случаях, установленных законодательством Российской Федерации, обязан обеспечить:

– предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

– своевременное обнаружение фактов несанкционированного доступа к информации;

– предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

– недопущение воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

– возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

– постоянный контроль за обеспечением уровня защищенности информации;

– нахождение на территории Российской Федерации баз данных информации, с использованием которых осуществляются сбор, запись, систематизация, накопление, хранение, уточнение (обновление, изменение), извлечение информации, необходимой для обеспечения деятельности университета.

2.6 Защита информации в информационной среде университета основывается на выявлении, оценке и противодействии возможным угрозам безопасности информации.

2.7 Основными видами угроз безопасности информации являются:

– противоправные действия внешних и внутренних нарушителей;

– ошибочные действия пользователей и обслуживающего персонала;

– отказы и сбои технических средств;

– вредоносные программные воздействия на информацию и средства информатизации, приводящие к её модификации, блокированию, уничтожению или копированию, а также нарушению правил эксплуатации средств вычислительной техники, вычислительных сетей, автоматизированных и информационных систем.

2.8 Реализация угроз безопасности информации сопровождается нарушением законных прав субъектов информационных отношений, причинением материального вреда.

2.9 Субъектами информационных отношений являются образовательные, научные, административно-управленческие, информационные и другие структурные подразделения университета, а также работники, обучающиеся и другие физические лица.

2.10 Обеспечение информационной безопасности, должно осуществляться в соответствии со следующими основными принципами:

– принцип законности: при организации и обеспечении защиты информации должно строго соблюдаться действующее законодательство Российской Федерации. Программные и программно-аппаратные средства, применяемые в университете, должны иметь соответствующие лицензии и сертификаты, официально приобретаться у представителей разработчиков этих

средств, в случаях требования законодательства иметь на них сертификаты безопасности. Организации, привлекаемые для проектирования, разработки, модернизации информационных (автоматизированных) систем, оказания других услуг в части защиты информации в случае требований законодательства должны иметь соответствующие лицензии на право ведения таких работ;

– принцип системности: при создании системы защиты информации должны учитываться актуальные угрозы безопасности информации, возможные объекты и направления атак на неё со стороны нарушителей. Система защиты информации должна строиться с учетом не только известных каналов утечки информации, несанкционированного доступа и воздействия на нее, но и с учетом возможности появления новых уязвимостей;

– принцип комплексности: комплексное использование средств защиты информации предполагает согласованное применение при построении целостной системы защиты, перекрывающей все существенные угрозы безопасности информации. Защита должна строиться эшелонировано. Физическая защита должна обеспечиваться физическими средствами и организационными мерами;

– принцип своевременности: разработка информационных систем и сервисов должна вестись одновременно с разработкой подсистемы защиты информации системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные информационные системы и сервисы, обладающие достаточным уровнем защищенности, позволит сэкономить финансовые средства;

– принцип преемственности: постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования информационных систем и системы её защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите информации;

– принцип достаточности: соответствие уровня затрат на обеспечение защиты информации и ценности информационных ресурсов на величину возможного ущерба от их разглашения, уничтожения и искажения. Используемые меры и средства защиты информации не должны ухудшать эргономические показатели компонентов информационных систем;

– принцип ответственности: возложение ответственности за обеспечение безопасности информации и её обработки на каждого работника и обучающегося в пределах их полномочий. В соответствии с этим принципом распределение прав и обязанностей работников и обучающихся строится таким образом, чтобы в случае любого нарушения был известен нарушитель;

– принцип обоснованности и технической реализуемости: информационные технологии, программные и программно-аппаратные средства, меры защиты информации должны быть реализованы

по современным решениям, обоснованы с точки зрения достижения заданного уровня защищенности информации и экономической целесообразности, а также соответствовать установленным нормам и требованиям по безопасности информации;

– принцип профессионализма: реализация мер защиты информации и эксплуатация средств защиты информации должна осуществляться профессиональными специалистами. Привлечение специализированных организаций к разработке средств и реализации мер защиты информации, подготовленных к конкретному виду деятельности по обеспечению безопасности информации, имеющих опыт практической работы и в случае требований законодательства соответствующие лицензии на право оказания услуг в этой области;

– принцип минимизации привилегий пользователей: обеспечение пользователей привилегиями минимально достаточными для выполнения ими своих должностных обязанностей. Исключение предоставления прав по умолчанию.

3 Организация защиты информации

3.1 Мероприятия по защите информации являются составной частью управленческой, научной, инновационной, учебной, производственной деятельности и проводятся в рамках единой комплексной системы защиты информации университета.

3.2 Для выполнения поставленных задач и достижения целей защиты информации принимаются правовые, организационные и технические меры.

3.3 Правовые меры включают в себя разработку на основе федеральных нормативных правовых актов локальных нормативных документов (актов), регулирующих вопросы защиты информации, применение этих документов (актов), а также контроль за их исполнением.

3.4 Организационные меры предусматривают:

– организацию и контроль доступа в контролируемую зону (учебные, административные корпуса, другие здания, защищаемые и другие помещения), к объектам информатизации;

– физическую защиту, охрану, в том числе техническими средствами и системой видеонаблюдения объектов информатизации (ОИ);

– режим доступа и работы на ОИ;

– разграничение прав доступа к информационным ресурсам, информационным системам и сервисам;

– порядок хранения, применения, передачи и уничтожения информации;

– другие меры.

Эти меры вводятся организационно-распорядительными и другими документами.

3.5 Меры по технической и криптографической защите информации включают использование программных, программно-аппаратных, аппаратных и криптографических средств для защиты информации в информационных системах, сервисах и телекоммуникационных сетях.

3.6 Управление системой защиты информации включает:

– внедрение и развитие локальной нормативной базы по защите информации;

– разработка и планирование мероприятий по защите информации;

– распределение обязанностей между подразделениями и работниками по обеспечению защиты информации;

– обучение персонала вопросам защиты информации;

– методическое обеспечение мероприятий по защите информации;

– управление рисками информационной безопасности.

3.7 Приказом ректора университета назначается ответственный за обеспечение информационной безопасности в университете (далее – ответственный за информационную безопасность, ответственный за ИБ), который отвечает, в том числе за обнаружение, предупреждение, ликвидацию последствий компьютерных атак и реагирование на компьютерные инциденты. Он обязан организовать в университете выполнение требований законодательства по обеспечению информационной безопасности. Он подчиняется непосредственно ректору, его указания и поручения в части обеспечения информационной безопасности являются обязательными для исполнения всеми работниками и обучающимися университета. Функциональные обязанности ответственного за информационную безопасность определяются федеральными нормативными актами и локальными актами, утвержденными ректором.

3.8 Общее и методическое руководство разработкой и организацией мероприятий по защите информации, их нормативное обеспечение и контроль за выполнением требований законодательства и локальных нормативных актов в области защиты информации, за эффективностью предусмотренных мер возлагается на отдел защиты информации управления внутренней безопасности университета (далее – отдел защиты информации, ОЗИ). Его функции определяются положением об отделе защиты информации, утвержденным ректором.

3.9 Экспертные функции по вопросам защиты информации выполняются экспертными комиссиями, рабочими группами, экспертами, должностными лицами, которые работают на основании приказа (распоряжения) ректора, распоряжений (поручений) ответственного за информационную безопасность (проректора по безопасности), проректоров.

3.10 Непосредственно организацию мероприятий по защите информации при создании, модернизации, эксплуатации объекта информатизации осуществляет руководитель структурного подразделения, отвечающего

за функционирование (создание, модернизацию, эксплуатацию) объекта информатизации, или другое должностное лицо, назначенное ректором (проректором).

3.11 Для проведения мероприятий по защите информации могут привлекаться на договорной основе специализированные организации, имеющие соответствующие лицензии на право проведения работ (оказание услуг) в области защиты информации.

3.12 Все мероприятия по разработке, созданию и модернизации объектов информатизации, изменению состава и конфигурации программных и технических средств, обрабатывающих конфиденциальную информацию, все мероприятия и изменения в организационно-технических решениях по защите информации, а также все разрабатываемые документы по организации защиты информации должны быть согласованы с ОЗИ.

3.13 Непосредственное руководство организацией и выполнением мероприятий по защите информации в структурных подразделениях возлагается на их руководителей.

3.14 Приказом ректора (директора филиала), распоряжением проректора, директора института (далее – приказ, распоряжение) назначаются ответственные за защиту информации в подразделениях. Они проводят работу и выполняют поручения руководителя подразделения, исходя из обязанностей руководителя подразделения в части организации защиты информации, делегируемых ему руководителем подразделения, взаимодействуют с ОЗИ.

3.15 Также приказом (распоряжением) в подразделениях назначаются ответственные за конфиденциальное делопроизводство, за защищаемые помещения и за другие объекты, процессы и мероприятия в подразделениях, обеспечивающие установленный порядок выполнения требований о защите информации. Указанные лица непосредственно организуют выполнение мероприятий по защите информации на порученных им участках работы, определенных настоящим Положением и другими нормативными и организационно-распорядительными документами, контролируют их выполнение работниками и обучающимися.

3.16 Обязанности по защите информации определяются Инструкцией по защите информации руководителю структурного подразделения университета (Приложение А), Инструкцией по защите информации работнику университета (Приложение Б), Инструкцией по защите информации обучающемуся университета (Приложение В), должностными инструкциями и другими нормативными и организационными документами.

3.17 Документы, определяющие требования о защите информации, доводятся под подпись в Журнале доведения до работников (обучающихся) требований о защите информации (далее – журнал доведения; Приложение Г) до всех работников в соответствии с занимаемой должностью при устройстве на работу (назначении на должность), до всех обучающихся – при поступлении

(зачислении) в университет; в последующем до всех работников и обучающихся – не реже одного раза в год, как правило, в начале учебного года.

Перечень документов, подлежащих доведению до работников и обучающихся, определяет отдел защиты информации.

Ответственность за доведение требований о защите информации возлагается: до работников - на руководителя структурного подразделения, до обучающихся – на лицо, назначенное директором института (филиала).

Запрещается допускать к работе лиц, не изучивших требования о защите информации.

3.18 Комплекс мероприятий по организации защиты информации в подразделении проводится в рамках системы защиты информации этого подразделения (локальной системы защиты информации, ЛСЗИ) во взаимодействии с ОЗИ на основании приказа (распоряжения).

3.19 Приказом (распоряжением) об организации защиты информации в подразделении:

- назначаются ответственные за защиту информации, за конфиденциальное делопроизводство, за защищаемые помещения в подразделении, за отдельные направления деятельности, процессы, проекты, мероприятия по защите информации, объекты информатизации;
- утверждаются списки информационных ресурсов, содержащих конфиденциальную информацию университета, информационных систем и сервисов, используемых в подразделении;
- утверждаются списки работников, допущенных к работе с конфиденциальной информацией и в информационных системах и сервисах;
- утверждаются списки защищаемых помещений (других объектов информатизации);
- определяются основные мероприятия по защите информации, сроки и ответственные за их выполнение;
- определяются другие вопросы по организации защиты информации.

Проект приказа (распоряжения) должен быть согласован с ОЗИ, копия приказа (распоряжения) направляется в ОЗИ.

4 Процесс защиты информации

Процесс защиты информации включает следующие процедуры:

4.1 Планирование мероприятий по организации защиты информации.

4.2 Мониторинг федеральной нормативной правовой базы по вопросам информационных технологий, защиты информации, документационного обеспечения управления и делопроизводства с целью выявления новых актов и внесенных изменений в действующие акты.

4.3 Формирование и актуализация локальной нормативной базы по защите информации на основе изменений федеральной нормативной

правовой базы и с учетом организационно-штатных и инфраструктурных изменений в университете.

4.4 Обеспечение подразделений нормативными и методическими документами по защите информации, другими рабочими материалами (журналами учета, бланками и т.п.).

4.5 Мониторинг инфраструктуры, информационной среды университета (организационно-штатная структура, информационные системы и сервисы, информационные ресурсы, учебные и административные корпуса, помещения, строения, информационно-телекоммуникационные системы, другие объекты информатизации, информационные технологии, процессы, проекты, мероприятия) с целью оценки ее защищенности от реализации угроз безопасности.

4.6 Анализ состояния системы защиты информации, защищенности информационной инфраструктуры, оценка рисков информационной безопасности. Разработка моделей угроз безопасности информации, оценка возможного причиненного вреда в результате реализации угроз безопасности.

4.7 Разработка требований по защите информации на автоматизированные и информационные системы, сервисы, вычислительные сети, средства вычислительной техники, другие объекты информатизации, передача их в подразделения для учета при планировании мероприятий и финансирования.

4.8 Разработка проектной и эксплуатационной документации в части защиты информации на автоматизированные и информационные системы, сервисы, вычислительные сети, средства вычислительной техники, другие объекты информатизации.

4.9 Разработка мероприятий по организации защиты информации в подразделениях, методическое руководство их выполнением.

4.10 Методическое руководство формированием структуры и сопровождением локальных систем защиты информации подразделений.

4.11 Организация подбора и подготовки персонала, привлекаемого к выполнению мероприятий по защите информации.

4.12 Нормативное и методическое обеспечение доведения до работников и обучающихся требований о защите информации.

4.13 Инвентаризация информационных систем и сервисов, информационных ресурсов в подразделениях, формирование (актуализация) списков информационных ресурсов, содержащих конфиденциальную информацию университета, информационных систем и сервисов, используемых в подразделениях (Приложение Д).

4.14 Организация и методическое сопровождение системы разграничения доступа к информационным системам и сервисам, конфиденциальной информации в подразделениях, формирование (актуализация) списков

работников, допущенных к работе с конфиденциальной информацией и в информационные системы и сервисы (Приложение Е).

4.15 Обследование учебных и административных корпусов, других строений, служебных помещений, формирование (актуализация) списков защищаемых помещений и ответственных за них в подразделениях (Приложение Ж).

4.16 Организация и поддержание в защищаемых и иных служебных помещениях режима допуска и работы, оформление технических паспортов на защищаемые помещения (Приложение И).

4.17 Организация и методическое сопровождение в подразделениях конфиденциального делопроизводства в соответствии с Инструкцией по конфиденциальному делопроизводству СФУ.

4.18 Разработка, утверждение и ввод в действие в установленном порядке организационных, распорядительных, методических документов по организации защиты информации.

4.19 Разработка и внедрение технических заданий на закупку, разработку, внедрение, модернизацию, эксплуатацию информационных систем, сервисов, СВТ, других технических средств обработки информации.

4.20 Планирование и проведение мероприятий по доведению уровня безопасности ИС и сервисов, ВС и СВТ до требуемого.

4.21 Разработка требований по защите информации в организационные документы подразделений (положения о подразделениях, должностные инструкции и др.), организационную и эксплуатационную документацию на ИС, ВС и СВТ (положения, регламенты, руководства и др.).

4.22 Разработка организационных и методических рекомендаций руководителям подразделений по организации (совершенствованию) системы защиты информации подразделения.

4.23 Инструкторско-методическая и профилактическая работа в подразделениях: доклады, занятия, инструктажи, консультации.

4.24 Оказание методической помощи подразделениям в выполнении мероприятий по защите информации.

4.25 Контроль выполнения требований по защите информации, а также эффективности предусмотренных мер защиты информации.

4.26 Проведение проверок и служебных расследований по инцидентам информационной безопасности, фактам нарушения требований защиты информации.

4.27 Взаимодействие с госструктурами по вопросам информационной безопасности (МОН, ФСТЭК, РКН, ФСБ и др.)

5 Порядок работы с конфиденциальной информацией

5.1 Порядок отнесения сведений к конфиденциальной информации, определения и изменения степени конфиденциальности документа (информации) определяется Инструкцией по конфиденциальному делопроизводству СФУ.

5.2 К работе с конфиденциальной информацией, в том числе персональными данными, допускаются работники университета, изучившие под подпись в журнале доведения настоящее положение, инструкцию по конфиденциальному делопроизводству СФУ, другие документы по защите информации. Перечень документов, подлежащих доведению, определяет ОЗИ.

5.3 Руководитель подразделения допускает к работе с конфиденциальной информацией, необходимой для исполнения служебных обязанностей, работников в соответствии со списком работников, допущенных к работе с конфиденциальной информацией, информационными системами и сервисами. Список утверждается ректором (проректором, директором института, филиала). В списке указывается, кто из работников и к какой конкретно информации допускается, их полномочия.

5.4 К работе с конфиденциальной информацией в другом подразделении университета работники допускаются по согласованию руководителей этих подразделений. Работник может быть включен в список в другом подразделении в соответствии с требованиями п. 5.3 настоящего Положения.

5.5 Лица, на которых возложены дополнительные обязанности приказом (распоряжением) ректора (лица, ответственные за делопроизводство, за материальные средства и др.), допускаются к работе с конфиденциальной информацией в подразделениях администрации университета на основании этого приказа (распоряжения) в пределах компетенции этого работника.

5.6 Полномочия по допуску к конфиденциальной информации членов советов, комиссий, рабочих групп и других постоянных или временных органов, а также отдельных должностных лиц определяются приказами, распоряжениями, положениями, должностными инструкциями или другими документами, регламентирующими работу этих органов (должностных лиц).

5.7 Уровень полномочий по доступу к конфиденциальной информации университета руководящего состава (проректоры, руководители департаментов, начальники управлений, директора филиалов и институтов), а также других должностных лиц в случаях, не определенных настоящим положением, определяется ректором, проректором, должностной инструкцией, другими организационными документами.

5.8 Обучающиеся допускаются к работе с конфиденциальной информацией в случаях необходимости привлечения их к мероприятиям и работам учебной, научной, служебной и другой деятельности в порядке, определенном для работников.

5.9 Передача информации включает ее распространение, доступ, предоставление. Порядок передачи персональных данных определяется Положением о персональных данных СФУ.

5.10 Распространение информации допускается в случаях, если она не является конфиденциальной. Документы с реквизитами СФУ (приказы, распоряжения, положения, инструкции, регламенты, стандарты и др.), не содержащие конфиденциальную информацию, могут распространяться или предоставляться в другие организации только с письменного разрешения ректора (проректора) или другого уполномоченного на это должностного лица.

5.11 Предоставление конфиденциальной информации сторонним организациям может осуществляться в виде зафиксированной на материальной основе, предоставлением возможности ознакомления с информацией уполномоченным лицам этих организаций или речевым сообщением.

5.12 Доступ к конфиденциальной информации осуществляется путем предоставления возможности получения информации из документов или соответствующих автоматизированных баз данных.

5.13 Конфиденциальная информация в правоохранительные, налоговые и другие органы государственной власти, местного самоуправления, в другие организации передается в порядке, установленном действующим законодательством.

5.14 Решение о передаче конфиденциальной информации третьей стороне принимается ректором (проректором по безопасности), который может запросить мнение экспертной комиссии (рабочей группы) или компетентных должностных лиц (специалистов) о возможности и целесообразности передачи конкретного объема конкретной информации.

5.15 Основанием для рассмотрения возможности и целесообразности передачи конфиденциальной информации является письменный мотивированный запрос (ходатайство) организации, который должен содержать:

– состав испрашиваемой информации;

– обоснование необходимости работы с этой информацией;

– ссылку на федеральный закон или другой нормативный правовой акт (с указанием конкретных статей), на основании которого запрашивается информация;

– форму передачи информации в соответствии с п. 5.11. настоящего Положения;

– представитель, уполномоченный на получение информации (фамилия, имя, отчество, серия и номер паспорта или служебного удостоверения, когда и кем выдан документ).

5.16 На основании резолюции ректора (проректора по безопасности) назначенным должностным лицом (подразделением) готовится информация для передачи или мотивированный отказ.

5.17 В случае принятия решения о передаче конфиденциальной информации с организацией, подавшей запрос (ходатайство), может быть заключено соглашение (договор) о порядке передачи и защите конфиденциальной информации.

5.18 При отношениях с партнерами и контрагентами защита конфиденциальной информации университета обеспечивается внесением во все стандартные формы договорной документации разделов о конфиденциальности. Объем сведений, признаваемых конфиденциальными, определяется в договоре.

5.19 Передача конфиденциальной информации может осуществляться на безвозмездной и возмездной основе, если это не противоречит законодательству, на основании требований нормативных правовых актов или в соответствии с соглашением сторон.

5.20 О передаче информации составляется акт или делается запись на запросе (мотивированном ходатайстве). В записи указывается дата передачи информации или дата уведомления об отказе в её предоставлении, а также отмечается, кому, какая именно информация была передана, форма передачи. Запись заверяется подписями лица, уполномоченного на передачу информации и уполномоченного представителя, получившего информацию.

5.21 Все работы с конфиденциальной информацией должны вестись только в защищаемых помещениях. Список защищаемых помещений подразделения утверждается ректором, проректором или директором института (филиала).

5.22 Все защищаемые помещения должны находиться в пределах контролируемой зоны, они должны контролироваться техническими средствами (охранно-пожарная сигнализация, видеонаблюдение, система управления и контроля доступа).

5.23 Физическая защита ЗП должна исключать несанкционированный доступ в них, нарушение работоспособности и хищение технических средств обработки, хранения и передачи информации, а также самой информации. Это обеспечивается оборудованием помещений надежными входными дверями, надежными замками, в том числе электронными или механическими кодовыми, механизмами, минимизирующими возможность случайного оставления их открытыми (доводчики закрытия дверей и т. п.), и другими необходимыми мерами.

5.24 В ЗП должен быть установлен режим доступа и работы, исключающий несанкционированный доступ в помещение и к обрабатываемой информации. Технические средства обработки информации должны быть закреплены за конкретными работниками. Мониторы, печатающие устройства, видеотерминалы, графопостроители, а также конфиденциальные документы должны размещаться так, чтобы исключался визуальный просмотр информации посторонними лицами (посетителями). При необходимости должны

применяться дополнительные меры, исключающие подобный просмотр (шторы, жалюзи, экраны и т. п.).

5.25 Порядок сдачи ЗП под охрану и снятия их с охраны определяется Правилами внутреннего распорядка СФУ, другими документами; для этого руководителем подразделения назначаются только работники, допущенные к работе с конфиденциальной информацией, и имеющие доступ в это ЗП.

5.26 Все контрольно-технические, ремонтные, строительные, хозяйственные работы, уборка в ЗП должны выполняться с разрешения (распоряжения) руководителя подразделения и под контролем ответственного за помещение или другого назначенного руководителем подразделения работника.

5.27 На ЗП руководитель подразделения (ответственный за защиту информации в подразделении, ответственный за ЗП) составляет Технический паспорт (Приложение И), который согласовывается с отделом защиты информации, и ведется ответственным за защиту информации в подразделении (ответственным за ЗП).

5.28 Для защиты речевой информации при ведении конфиденциальных переговоров, совещаний, предотвращения утечки информации в акустическом канале целесообразно принимать меры по ограничению допуска к объектам защиты, повышению их звукоизоляции; могут проводиться проверки на наличие закладочных устройств несанкционированного прослушивания (радиомикрофоны, диктофоны и другие технические средства).

5.29 Запрещается проведение любых мероприятий и работ с использованием сведений конфиденциального характера без принятия необходимых мер защиты информации.

5.30 Защита информации в процессе ведения делопроизводства и служебной переписки обеспечивается точным соблюдением требований нормативных документов, регламентирующих ведение делопроизводства. Порядок ведения конфиденциального делопроизводства определяется Инструкцией по конфиденциальному делопроизводству СФУ.

6 Защита информации, обрабатываемой в информационных системах и сервисах

6.1 Защита информации, обрабатываемой с использованием информационных систем (ИС), автоматизированных систем (АС), вычислительных сетей (ВС), сервисов и СВТ (далее – информационные системы и сервисы, ИС), является составной частью работ по созданию, модернизации и эксплуатации этих средств; она должна реализовываться посредством системы (подсистемы) защиты информации (СЗИ) и предусматривать комплекс организационных, технических (аппаратных, программных, аппаратно-

программных) и криптографических средств, и мер при ее автоматизированной обработке, хранении и передаче по каналам связи.

6.2 Организация защиты информации в информационных системах и сервисах возлагается на руководителей подразделений, сопровождающих эти системы; могут также назначаться штатные или нештатные администраторы безопасности (защиты) информации, наделенные необходимыми полномочиями; эти полномочия могут возлагаться на других сотрудников, специалистов (администраторы ИС, сетевые администраторы и др.).

6.3 Все компоненты информационных систем (стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования информационной системы) должны размещаться в защищаемых помещениях в пределах контролируемой зоны. Контролируемая зона включает пространство (территорию, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание работников, обучающихся и лиц, не имеющих постоянного допуска на объекты университета (не являющихся работниками и обучающимися университета), а также транспортных, технических и иных материальных средств.

6.4 Контролируемая зона в университете определяется границами (стенами) зданий, сооружений университета, нахождение в которой контролируется службами безопасности, должностными лицами, техническими средствами охраны, в т.ч. системами видеонаблюдения, контроля и управления доступом.

6.5 Мероприятия по ЗИ в информационных системах должны проводиться на всех стадиях жизненного цикла ИС с учетом требований законодательства, нормативных актов и методических документов в области ЗИ.

6.6 Для обработки информации, необходимость защиты которой определяется законодательством Российской Федерации, должны использоваться информационные системы, обладающие функциями автоматизированных систем в защищенном исполнении (АСЗИ), в которых реализованы в соответствии с действующим законодательством требования о защите информации.

6.7 Реализация требований о защите информации в ИС осуществляется посредством системы защиты информации (СЗИ), являющейся неотъемлемой составной частью ИС. Требования к защите информации формируются в зависимости от уровня (класса) защищенности ИС, угроз безопасности информации, структурно функциональных характеристик информационной системы, применяемых информационных технологий информационной системы.

6.8 СЗИ ИС должна обеспечивать комплексное решение задач по ЗИ от НСД, от утечки защищаемой информации по техническим каналам, от несанкционированных и непреднамеренных воздействий на информацию

(на носители информации) применительно к конкретной ИС. Состав решаемых задач по ЗИ определяется задачами обработки информации, решаемыми с использованием ИС, ее программным и аппаратным составом, конфигурацией этой системы, условиями функционирования, требованиями, предъявляемыми к обрабатываемой информации, угрозами безопасности информации.

6.9 Создание (модернизация) и эксплуатация ИС должны осуществляться с учетом требований законодательства и нормативных документов по защите информации. Требования по защите информации, предъявляемые к ИС, задаются в ТЗ на создание системы в виде отдельного подраздела ТЗ «Требования по защите информации». ТЗ на проектирование ИС, проектная и другая техническая и эксплуатационная документация в обязательном порядке должны быть согласованы с ОЗИ.

6.10 При модернизации ИС, предназначенной для обработки конфиденциальной информации, должно разрабатываться ТЗ на создание СЗИ или дополнение к основному ТЗ на ИС, в которое включают требования к СЗИ, а также к той части ИС, которая подлежит доработке (модернизации) в связи с включением в состав ИС системы ЗИ.

6.11 В ИС защите подлежат:

- информационные ресурсы в виде информационных массивов и баз данных, содержащих защищаемую информацию, и представленные на магнитных, оптических и других носителях;
- средства автоматизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и прикладное программное обеспечение).

6.12 Подразделения, обеспечивающие эксплуатацию информационных систем, должны проводить мероприятия и принимать меры по защите информации в ходе сопровождения, обслуживания информационных систем, поставки комплектующих и иных видов работ по эксплуатации информационных систем.

6.13 В ИС должны применяться серийно выпускаемые или специальные (разрабатываемые в ходе создания ИС) технические и программные средства обработки информации, а также технические, программные, программно-аппаратные, криптографические средства защиты информации и средства контроля эффективности ЗИ. Средства защиты информации, применяемые в ИС, должны пройти оценку соответствия в порядке, определенном законодательством.

6.14 На СВТ должна быть жестко определена конфигурация ПО, запрещается ее несанкционированное изменение, использование нелицензионного программного обеспечения, а также ПО, которое не предназначено для служебных целей.

Мероприятия по контролю конфигураций информационных систем должны исключать несанкционированное изменение состава программных, программно-аппаратных средств информационных систем, их настроек и конфигураций.

6.15 В случаях, установленных законодательством, осуществляется аттестация ИС на соответствие требованиям безопасности информации в соответствии с положениями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов.

6.16 Предотвращение НСД к информации обеспечивается разграничением и управлением доступа пользователей к ресурсам информационных систем, применением специальных программно-аппаратных средств защиты, использованием криптографических средств защиты информации и другими организационными и техническими мероприятиями.

6.17 Разграничение доступа пользователей к ресурсам информационных систем реализуется конфигурированием и настройкой сетевого оборудования, межсетевых экранов, созданием матриц доступа пользователей к серверам и рабочим станциям и их ресурсам, установкой соответствующих разрешений в настройках операционных систем, другими мерами и средствами.

6.18 Управление доступом подразумевает управление идентификацией и аутентификацией пользователей, управление присвоением им прав и привилегий по доступу к ресурсам, контроль доступа и выявление попыток НСД. При доступе в информационную систему должна осуществляться идентификация и аутентификация пользователей, являющихся работниками и обучающимися университета (внутренних пользователей), и процессов, запускаемых от имени этих пользователей, а также процессов, запускаемых от имени системных учетных записей.

6.19 Идентификация и аутентификация пользователей обеспечивается использованием уникальных имени пользователя (идентификатора) и пароля, аппаратных идентификаторов (электронные замки и ключи, смарт-карты, биометрические устройства и другие) и другими методами.

6.20 Парольная защита при работе на СВТ, в ИС и ВС осуществляется с целью предотвращения несанкционированного доступа (НСД) к информации, она является составной частью подсистемы управления доступом общей системы защиты от НСД.

6.21 Вход в операционные системы ПЭВМ, другие СВТ, ВС, ИС должен быть ограничен паролем. Конфиденциальная информация должна храниться в ПЭВМ только в базах и банках данных, папках и файлах, вход в которые ограничен паролем. Требования к организации парольной защиты определяются инструкцией (Приложение К).

6.22 Запрещается подключение ИС, ВС и отдельных ПЭВМ, обрабатывающих конфиденциальную информацию, к сети Интернет и к другим

информационным системам и сетям без использования специальных сертифицированных технических и криптографических средств защиты информации (межсетевые экраны и др.).

6.23 Для передачи информации по каналам связи, выходящим за пределы КЗ, необходимо использовать защищенные каналы связи или предназначенные для этого криптографические средства защиты информации.

6.24 Обработка служебной информации, в том числе неконфиденциальной, должна вестись только в ИС и сервисах, включенных в список информационных систем и сервисов подразделения, утвержденный приказом (распоряжением) ректора, распоряжением проректора, директора института (филиала).

6.25 Категорически запрещается хранить, обрабатывать и передавать служебную информацию, в том числе неконфиденциальную, в некорпоративных системах и сервисах (электронная почта, мессенджеры, облачные технологии и др.).

6.26 Запрещается передавать конфиденциальную информацию по электронной почте, телефону, факсу, национальному мессенджеру.

6.27 Обмен конфиденциальной информацией между отдельными автоматизированными рабочими местами (АРМ) может осуществляться с помощью съемных носителей информации с учетом допуска исполнителей, работающих на АРМ, к переносимой информации. При этом должны соблюдаться меры безопасности: носители должны быть учтены и храниться установленным порядком, информация должна пройти антивирусный контроль, должна быть закрыта паролем и др.

6.28 Предотвращение вредоносных программно-математических воздействий, вызывающих уничтожение, искажение информации или сбои в работе средств информатизации, обеспечивается применением специальных программных и аппаратных средств защиты (антивирусные процессоры, программы), средств криптографической защиты информации, контролем целостности программной среды ИС и СВТ, постоянным антивирусным контролем.

6.29 Меры по антивирусной защите должны обеспечивать обнаружение в информационных системах компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации. Должно быть обеспечено обновление баз данных признаков вредоносных компьютерных программ (вирусов).

6.30 Для антивирусной защиты должны использоваться только лицензионные программные антивирусные средства.

6.31 Установка средств антивирусной защиты должна осуществляться

специалистами ДИТ или специалистами других подразделений, сопровождающих ИС, допущенными к этим работам установленным порядком.

6.32 Пользователь ИС должен перед началом работы проверить обновление антивирусной базы. Все внешние носители информации (флеш-накопители, жесткие диски и др.) перед использованием должны проверяться на наличие компьютерных вирусов.

6.33 При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) пользователь ИС должен самостоятельно или вместе с администратором провести внеочередной антивирусный контроль или обратиться в сервисную службу ИТ-запросов ДИТ.

6.34 При обнаружении компьютерного вируса пользователь ИС обязан приостановить использование АРМ, немедленно поставить в известность о факте обнаружения зараженных вирусом файлов ДИТ и действовать по указанию специалиста ДИТ.

6.35 В информационной системе должны обеспечиваться резервное копирование данных, резервирование технических средств, программного обеспечения, каналов передачи данных, средств обеспечения ИС в соответствии с требованиями руководящих документов.

Периодичность резервного копирования, количество, типы носителей, места хранения резервных копий и уровень критичности резервируемой информации определяются руководителями подразделений, сопровождающими ИС.

6.36 В подразделениях порядок резервирования служебной информации (рабочей, важной), в том числе неконфиденциальной, определяет руководитель подразделения.

6.37 В подразделении, сопровождающим ИС, должен быть обеспечен учет машинных носителей информации, используемых в информационной системе для хранения и обработки информации. Учету подлежат:

- съемные машинные носители информации (флэш-накопители, внешние накопители на жестких дисках и иные устройства);
- портативные вычислительные устройства, имеющие встроенные носители информации (ноутбуки, нетбуки, планшеты, сотовые телефоны, цифровые камеры, звукозаписывающие устройства и иные аналогичные по функциональности устройства);
- машинные носители информации, встроенные в корпус средств вычислительной техники (накопители на жестких дисках).

6.38 Порядок учета, хранения, движения, уничтожения съемных машинных (электронных) носителей информации определяется Инструкцией по конфиденциальному делопроизводству СФУ.

6.39 Должны быть обеспечены регламентация и контроль использования мобильных технических средств, направленные на защиту информации в информационной системе, должны приниматься меры по защите информационных систем и содержащейся в них информации, в том числе: обеспечивать защиту каналов передачи данных и осуществлять доступ пользователей с применением строгой аутентификации.

Пользователь должен обеспечить исключение несанкционированного доступа к мобильному устройству.

6.40 Использование мобильных электронных устройств при проведении служебных совещаний, конференций, собраний, учебных занятий и других мероприятий в помещениях университета допускается только с разрешения руководителя подразделения или проводимого мероприятия. Руководитель, проводящий конфиденциальное мероприятие, обязан предупредить присутствующих об отключении мобильных средств связи, а при необходимости и других устройств.

6.41 Электропитание технических средств обработки информации целесообразно осуществлять через развязывающие фильтры и с использованием источников бесперебойного питания. Серверы, активное сетевое оборудование, а также наиболее важные рабочие станции целесообразно обеспечивать резервными линиями электропитания, автономными источниками резервного электропитания.

6.42 При удаленном доступе пользователей к информационным системам в целях выполнения своих обязанностей (функций) должны приниматься меры по защите информационных систем и содержащейся в них информации, обеспечиваться защита каналов передачи данных и программно-аппаратных средств, с использованием которых осуществляется удаленный доступ, исключаться несанкционированный доступ к удаленно подключаемому программно-аппаратному средству пользователя.

6.43 Права удаленного доступа предоставляются пользователям на основании списка, утвержденного ректором, проректором, директором института (филиала). Количество пользователей с удаленным доступом должно быть строго ограничено, им назначаются минимально необходимые права и привилегии при удаленной работе.

7 Управление рисками информационной безопасности

С целью управления рисками информационной безопасности планируются и проводятся следующие мероприятия:

7.1 Мониторинг:

- федеральной нормативной правовой и методической базы по информационной безопасности;

- информационной инфраструктуры университета (организационная структура, информационные ресурсы, ИС, АС, ВС, сервисы, СВТ, ПО, служебные помещения, делопроизводство, другие объекты информатизации);

- производственной деятельности, информационных технологий (текущий контроль, плановые и неплановые проверки, служебные проверки и расследования по инцидентам информационной безопасности).

7.2 Анализ угроз и оценка рисков:

- анализ соответствия локальных нормативных актов по защите информации требованиям федеральных нормативных правовых актов;

- выявление угроз, уязвимостей информационных систем, рисков, уровней защищенности информации;

- оценка вероятности реализации угроз безопасности, масштаба последствий, определение возможных убытков.

7.3 Выбор и разработка мероприятий:

- по оперативной минимизации возможного ущерба при инцидентах информационной безопасности;

- по устранению недостатков, способствующих реализации нарушений;

- по актуализации локальных нормативных актов и других документов с целью приведения их в соответствие с федеральными актами;

- по закрытию каналов утечки информации и несанкционированного доступа к информации.

7.4 Оценка принятых мер, совершенствование системы и методологии защиты информации.

7.5 В случае нарушения технологии обработки конфиденциальной и другой защищаемой информации, угрозе её безопасности проректор по безопасности по представлению начальника управления внутренней безопасности (начальника ОЗИ), руководителя департамента информационных технологий имеет право приостанавливать работы на объекте, извещая руководителя подразделения, сопровождающего и эксплуатирующего этот объект. По фактам нарушений проводится проверка или служебное расследование. Эксплуатация объекта возобновляется после принятия решения по данному вопросу ректором (проректором по безопасности).

7.6 Взаимодействие с вышестоящими организациями в системе высшей школы, а также с другими учреждениями и организациями в интересах защиты информации университета осуществляют проректор по безопасности, начальник управления внутренней безопасности, начальник ОЗИ, руководитель департамента информационных технологий и другие лица по поручению ректора (проректора по безопасности).

8 Реагирование на инциденты информационной безопасности, на угрозы безопасности информации и предпосылки к ним

8.1 К инцидентам информационной безопасности, угрозам безопасности и предпосылкам к ним (далее – инциденты безопасности) относятся:

– заражение средств вычислительной техники вредоносными программами, нарушение работоспособности и сбои в работе технических средств, отказ оборудования, сервисов, средств обработки и (или) защиты информации;

– несанкционированное изменение в конфигурацию программных и аппаратных средств обработки и защиты информации, изменение настроек, состава, паролей средств вычислительной техники, очистка электронных журналов мониторинга и др.;

– использование средств вычислительной техники и других технических средств в целях, несвязанных с выполнением служебных обязанностей;

– другие факты (попытки) нарушений работы технических средств обработки информации и правил работы в информационных системах и сервисах.

– сеансы работы в информационных системах незарегистрированных пользователей, пользователей с нарушением установленного времени доступа, пользователей, срок действия полномочий которых истек, либо в состав предоставленных ему полномочий, которых не входит работа в информационных системах и сервисах;

– факты и попытки совершения противоправных действий при работе в информационных системах и сервисах (несанкционированный доступ к конфиденциальной информации, к информационным системам и сервисам, к элементам инфраструктуры, обеспечивающих безопасность обработки персональных данных, в защищаемые помещения и другие противоправные действия);

– нарушение конфиденциальности, целостности, доступности конфиденциальной информации;

– нарушение целостности и доступности открытой (общедоступной) информации;

– утрата (хищение) конфиденциальных документов, носителей персональных данных, криптосредств, ключевых документов, личных печатей, удостоверений, пропусков.

8.2 Управление инцидентами информационной безопасности (далее – инциденты) предусматривает следующие стадии:

– организация деятельности по управлению инцидентами;

– обнаружение и регистрация инцидентов;

– реагирование на инциденты;

– анализ результатов деятельности по управлению инцидентами.

8.2.1 Организация деятельности по управлению инцидентами.

8.2.2 Обнаружение и регистрация инцидентов основывается на результатах проводимого в университете мониторинга информационной безопасности, в рамках которого осуществляется сбор информации о событиях безопасности и иных данных мониторинга из различных источников.

Регистрация признаков возможного возникновения инцидентов может осуществляться как автоматизированным способом на основе правил регистрации признаков возможного возникновения инцидентов, так и неавтоматизированным способом (специалистами ДИТ и ОЗИ, руководителями подразделений, пользователями ИС и сервисов).

Подтверждение инцидента осуществляется в ходе проверки признака возможного возникновения инцидента. Такая проверка проводится специалистами ДИТ, ОЗИ, других подразделений, ответственными за реагирование на компьютерные инциденты (ответственными за защиту информации в подразделениях, администраторами систем и сервисов, руководителями рабочих групп реагирования на инциденты и др.).

8.2.3 Реагирование на компьютерные инциденты

Стадия состоит из следующих последовательных этапов:

– определение вовлеченных в инцидент элементов информационной инфраструктуры с целью их дальнейшей локализации;

– локализация компьютерного инцидента, направленная на ограничение функционирования элементов информационной инфраструктуры, вовлеченных в инцидент, с целью предотвращения его дальнейшего распространения (применение блокировок, использование межсетевого экрана, отключение, выключение, изменения маршрутизации, отключение или блокирование процессов, отключение учетных записей пользователей);

– выявление последствий инцидента: действия, направленные на выявление признаков негативного воздействия на элементы информационной инфраструктуры, вовлеченные в инцидент, проведение детального анализа имеющихся данных о компьютерном инциденте;

– ликвидация последствий инцидента: действия, направленные на устранение последствий негативного влияния инцидента на информационный ресурс (по возможности) и/или восстановление элемента информационной инфраструктуры (группы элементов или информационного ресурса в целом), и/или обрабатываемой в нем информации;

– закрытие инцидента по результатам проверки руководителем рабочей группы реагирования на инцидент, в ходе которой определяется полнота выполненных действий по реагированию на инцидент, выполненных на каждом этапе реагирования на инцидент.

8.2.4 Анализ результатов деятельности по управлению инцидентами:

– установление причин и условий возникновения инцидентов;

– изучение опыта по результатам управления инцидентами;

– разработка рекомендаций по устранению в информационных ресурсах причин и условий возникновения инцидентов;

– оценка результатов и эффективности реагирования на инциденты.

8.3 Работу по реагированию на инциденты организует руководитель ДИТ во взаимодействии с начальником ОЗИ.

8.4 Инциденты безопасности могут быть выявлены (допущены) пользователями информационных систем и сервисов (далее – пользователи), а также другими лицами в ходе работы, текущего контроля, плановых и неплановых проверок. В случае выявления инцидента безопасности пользователь обязан прекратить работу с ресурсом, в котором выявлен инцидент, сообщить об инциденте в отдел управления ИТ-запросами ДИТ и руководителю структурного подразделения. Руководители отдела управления ИТ-запросами ДИТ и подразделения должны доложить об инциденте руководителю ДИТ и начальнику ОЗИ.

8.5 Руководитель ДИТ при необходимости во взаимодействии с начальником ОЗИ формирует оперативную группу, которая проводит анализ ситуации и причин инцидента, принимает оперативные контрмеры для локализации инцидента. Результаты работы излагаются в письменном докладе ответственному за информационную безопасность в университете (проректору по безопасности), который принимает решение о дальнейших действиях по факту инцидента.

8.6 При необходимости приказом (распоряжением) ректора назначается комиссия по расследованию инцидента, в которую входят проректор по безопасности (председатель комиссии), руководитель ДИТ, начальник ОЗИ, другие компетентные специалисты, эксперты. Установленным порядком проводится расследование, которое должно установить факт инцидента, обстоятельства, причины его возникновения, виновные лица и степень их вины, причиненный ущерб (при наличии), его оценка, меры, принятые для ликвидации последствий, другие вопросы. По окончании расследования комиссия представляет ректору акт расследования, по которому принимается решение. Материалы расследования инцидента являются конфиденциальными.

8.7 В случае, если инцидент безопасности может стать (или уже стал) причиной негативных последствий, необходимо немедленно прекратить работу в ИС и сервисе, по возможности блокировать доступ к этим сервисам до устранения причин, повлекших наступление инцидента безопасности и его последствий. Решение о блокировании доступа к ИС и сервисам принимает ректор или ответственный за информационную безопасность в университете (проректор по безопасности), а в исключительных случаях – руководитель ДИТ.

8.8 На основании действующего законодательства могут приниматься другие меры по фактам выявленных инцидентов и возможным угрозам информационной безопасности.

9 Организация внутреннего контроля

9.1 Контроль выполнения требований по защите информации, достаточности и эффективности предусмотренных мер защиты информации является процедурой (составной частью) процесса защиты информации.

9.2 За организацию внутреннего контроля в университете отвечает ответственный за обеспечение информационной безопасности в университете (проректор по безопасности; далее – ответственный за информационную безопасность, ответственный за ИБ).

9.3 Непосредственно внутренний контроль организует и проводит отдел защиты информации. По распоряжению (указанию) ответственного за информационную безопасность для контроля могут привлекаться другие подразделения университета, должностные лица, сотрудники, а также на договорной основе сторонние организации, имеющие на это право в соответствии с требованиями законодательства.

9.4 Задачи контроля:

– проверка состояния организации защиты информации в проверяемом подразделении: наличие и актуальность необходимых организационных документов, назначение ответственных за мероприятия по вопросам защиты информации, доведение до работников требований по защите информации, других необходимых документов;

– проверка соответствия мероприятий по защите информации требованиям федеральных нормативных правовых и локальных нормативных актов;

– проверка своевременности и полноты выполнения требований руководящих документов, регламентирующих организацию и порядок осуществления мероприятий по защите информации;

– выявление внутренних угроз информационной безопасности, исходящих от работников и обучающихся университета; предупреждение и пресечение правонарушений в части защиты информации работниками или обучающимися университета;

– оценка обоснованности, достаточности и эффективности предусмотренных мер защиты информации.

9.5 Внутренний контроль включает текущие (периодические), плановые и внеплановые проверки.

9.6 Текущие (периодические) проверки проводятся руководителями структурных подразделений и ответственными работниками в подразделениях, назначенными приказом (распоряжением), ответственными за сопровождение

и безопасность ИС, за другие объекты информатизации, рабочие процессы, проекты, мероприятия, а также сотрудниками ОЗИ в процессе управленческой, образовательной, научной, инновационной, производственной и другой деятельности подразделений университета.

9.7 Плановые проверки проводятся сотрудниками ОЗИ, назначенными комиссиями, должностными лицами в соответствии с утвержденным планом работы и графиком проверки подразделений на текущий год. Плановые проверки подразделений проводятся не реже одного раза в три года.

9.8 Внеплановые проверки могут проводиться в следующих случаях:

– при расследовании инцидентов информационной безопасности;

– по результатам внешних контрольных мероприятий, проводимых регулирующими органами;

– в других случаях по решению ректора или ответственного за информационную безопасность в университете (проректора по безопасности).

9.9 Внутреннему контролю подлежат структурные подразделения, информационные системы и сервисы, другие объекты информатизации, а также отдельные функции, рабочие процессы, проекты, мероприятия, проводимые в подразделениях в ходе управленческой, образовательной, научной, инновационной, производственной и другой деятельности в части организации и состояния защиты информации.

9.10 Допуск лиц к проведению контроля за состоянием защиты информации производится на основании приказа или распоряжения ректора (проректора по безопасности), а также в соответствии с должностными инструкциями. Начальник управления внутренней безопасности, сотрудники ОЗИ допускаются к проведению контроля во всех подразделениях, информационных системах и сервисах университета беспрепятственно в пределах своих должностных обязанностей. Проректоры и руководители подразделений имеют право на проверку подчиненных им подразделений и объектов.

9.11 При проведении плановых проверок не позднее, чем за три рабочих дня до начала проведения проверки руководитель структурного подразделения (ответственный за объект информатизации, за процесс, за мероприятие), подлежащего проверке, письменно уведомляется о предстоящей проверке с приложением программы проверки.

В уведомлении должны быть указаны дата, время, продолжительность, цель и задача проверки, объекты (подразделения, ИС и сервисы, процессы, мероприятия), уполномоченные лица на проведение проверки.

При проведении текущего (периодического) контроля и внеплановых проверок уведомление не требуется.

9.12 При плановом контроле проверяется:

– наличие и актуальность организационно-распорядительных и других документов по организации защиты информации;

– доведение до работников под подпись требований по защите информации, нормативных и организационно-распорядительных документов;

– организация разграничения прав и полномочий работников по доступу к информации, информационным системам и сервисам, в т.ч. к базам данных и программному обеспечению ИС и их элементов;

– учет и хранение носителей информации;

– порядок, технология обработки конфиденциальной и другой информации, в т.ч. автоматизированной;

– соблюдение работниками требований по защите информации при работе в ИС и сервисах;

– наличие и порядок применения средств защиты информации;

– наличие (отсутствие) инцидентов информационной безопасности и принятие необходимых мер;

– вопросы технической надежности аппаратно-программных средств обработки и защиты информации.

9.13 Проверка проводится изучением документов, опросом работников, обследованием (осмотром) помещений, объектов, рабочих мест, СВТ и средств защиты информации, мониторингом вычислительных сетей, порядка и мест хранения носителей информации, другими методами.

9.14 При проведении контроля также:

– изучаются функции, рабочие процессы, проекты, мероприятия, проводимые в подразделении с целью выявления возможных угроз безопасности информации для разработки мер по их нейтрализации;

– оказывается помощь работникам подразделения оперативно устранить выявленные недостатки и нарушения;

– непосредственно на рабочих местах инструктируется персонал по выполнению требований по защите информации;

– совместно с руководством подразделения выявляются проблемы в части защиты информации, намечаются пути их решения.

9.15 В особых случаях, когда проверка непосредственно в подразделении невозможна или нецелесообразна (карантин, чрезвычайные ситуации и др.), проверка может проводиться дистанционно запросом документов для изучения и оценки вопросов организации и состояния защиты информации, мониторингом информационной инфраструктуры подразделений и объектов, вычислительных сетей, дистанционным опросом работников (только корпоративные сервисы: ИС, телефон, электронная почта и др.).

9.16 Руководители структурных подразделений и все другие работники университета во всех случаях обязаны представить сотрудникам ОЗИ все необходимые документы, материалы и сведения, кроме сведений, составляющих государственную тайну, а также обеспечить доступ в помещения,

к информационным системам и сервисам, другим техническим средствам обработки и защиты информации.

9.17 По результатам контроля даётся оценка состояния работ и эффективности принятых мер защиты информации. Защита информации считается эффективной, если принимаемые меры обеспечивают реализацию заданных целей, замыслов, требований и соответствуют установленным нормам.

9.18 Результаты контроля (плановые и неплановые проверки) отображаются в акте проверки, дается оценка состояния работ и эффективности технологии обработки информации и принятых мер по ее защите. Акт подписывается работниками, проводившими проверку, утверждается ректором (проректором по безопасности).

По результатам текущего (периодического) контроля могут составляться справки, доклады, акты.

9.19 Акт проверки хранится в отделе защиты информации, а копия акта направляется руководителю проверенного подразделения (объекта, процесса, мероприятия). Копия акта может направляться другим должностным лицам (курирующему проректору и др.). Отдел защиты информации разрабатывает и направляет в проверенное подразделение рекомендации и методические указания по устранению выявленных нарушений, совершенствованию технологии обработки и защиты информации, по другим вопросам, предусмотренным требованиями федеральных и локальных нормативных правовых актов.

9.20 Внешний контроль (аудит, мониторинг, тестирование и т.п.) проводятся в соответствии с требованиями законодательства, федеральных нормативных актов.

10 Заключительные положения

10.1 Финансирование мероприятий по защите информации предусматривается в бюджете университета в соответствии с утверждённым перечнем мероприятий на очередной год и сроками их выполнения.

10.2 Расходы на создание (модернизацию) систем защиты информации объектов информатизации включаются в смету расходов на создание (модернизацию) этих объектов информатизации.

10.3 Персональная ответственность за невыполнение установленных правил по защите информации на объекте информатизации (в подразделении) возлагается на ответственного за этот объект (руководителя подразделения), а непосредственно на рабочем месте – на работника, эксплуатирующего это рабочее место.

10.4 Лица, виновные в нарушении норм, регулирующих обработку и защиту конфиденциальной информации, несут дисциплинарную,

административную, гражданско-правовую или уголовную ответственность в соответствии с действующим законодательством РФ.

10.5 Положение пересматривается в случае возникновения несоответствий с нормативными правовыми актами РФ, по мере развития информационной среды университета, совершенствования ее программно-технического обеспечения и информационных технологий.

10.6 Право инициативы внесения изменений и дополнений в положение предоставляется ректору, проректорам, начальнику УВБ, начальнику ОЗИ и руководителям структурных подразделений.

10.7 Предложения о внесении изменений и дополнений в положение оформляются в виде служебной записки на имя проректора по безопасности с обоснованием такой необходимости.

10.8 Предложение о внесении изменений и дополнений в положение рассматривается назначенной ректором (проректором по безопасности) комиссией или рабочей группой. В случае необходимости к работе могут быть дополнительно привлечены эксперты, специалисты.

10.9 Проект положения в новой редакции представляется для утверждения ректору. Положение вступает в силу с момента утверждения его приказом ректора.

РАЗРАБОТЧИК

Начальник ОЗИ	А.Ф. Курбатов

СОГЛАСОВАНО

Проректор по перспективным проектам	С.В. Верховец
Проректор по УР	Д.С. Гуц
Проректор по НР	Д.В. Капулин
Проректор по ИП	Е.А. Туртапкина
Проректор по безопасности	П.А. Юдин
Директор АПД	Н.В. Самарникова
Начальник УВБ	А.В. Лунёв
Нормоконтролер: начальник ОСОРД	Л.А. Пяткова

ПРИЛОЖЕНИЕ А

Инструкция по защите информации руководителю структурного подразделения СФУ

Руководитель структурного подразделения отвечает за организацию и проведение мероприятий по защите информации в подразделении и выполнение всех требований нормативных документов по защите информации работниками (обучающимися) подразделения.

Руководитель подразделения обязан:

1 Знать и строго выполнять требования локальных нормативных актов, других документов по защите информации; во взаимодействии с ОЗИ организовать и обеспечить функционирование системы защиты информации подразделения; все разрабатываемые документы, касающиеся вопросов защиты информации, согласовывать с ОЗИ.

2 Определять ответственному за защиту информации в подразделении его функции, исходя из своих обязанностей в части организации защиты информации.

3 Требовать от работников (обучающихся) подразделения выполнения требований по защите информации и контролировать выполнение.

4 Готовить проект приказа (распоряжения) об организации защиты информации и другие необходимые документы, издавать (утверждать) их установленным порядком; при изменениях в организационной и инфраструктуре, кадровых изменениях своевременно вносить изменения в эти документы.

5 В соответствии с Перечнем сведений, составляющих конфиденциальную информацию СФУ, и номенклатурой дел подразделения формировать и периодически уточнять в подразделении Список информационных ресурсов подразделения, содержащих конфиденциальную информацию СФУ, информационных систем и сервисов, и утверждать его установленным порядком.

6 Осуществлять подбор работников для допуска к работе с конфиденциальной информацией, определять им необходимые для работы ИС и сервисы, информацию, в каком объеме и с какими правами они допускаются для исполнения служебных обязанностей. Формировать Список работников подразделения, допущенных к работе с конфиденциальной информацией, информационными системами и сервисами, утверждать его установленным порядком.

7 Допускать в соответствии с утвержденным Списком к работе с конфиденциальной информацией, информационными системами и сервисами, необходимыми для исполнения служебных обязанностей, работников, изучивших требования нормативных документов по защите информации.

8 Определять в каких помещениях есть служебная необходимость хранить и обрабатывать конфиденциальную информацию, размещать АРМ, СВТ, элементы информационных систем и сервисов, формировать Список защищаемых помещений подразделения и ответственных за них, утверждать его установленным порядком.

9 Организовать и поддерживать в подразделении режим допуска в защищаемые помещения, к ИС и сервисам, другим техническим средствам и к информационным ресурсам. Назначать установленным порядком ответственных за защищаемые помещения и лиц, допущенных к их вскрытию (закрытию). Оформлять технические паспорта на защищаемые помещения, поддерживать их в актуальном состоянии, своевременно вносить в них изменения.

10 Закреплять за работниками подразделения автоматизированные рабочие места, средства вычислительной техники и другие технические средства обработки и передачи информации, следить за их правильной эксплуатацией.

11 Допускать работников к исполнению служебных обязанностей только после изучения ими Инструкции работнику (руководителю структурного подразделения) по защите информации, Перечня сведений, составляющих конфиденциальную информацию СФУ и других документов по согласованию с ОЗИ, в дальнейшем документы доводить не реже одного раза в год.

12 Определять работникам задачи и обязанности, организовывать проведение инструктажей и занятий с ними по вопросам защиты информации, прививать им правила и нормы служебной этики, направленные на обеспечение информационной безопасности.

13 Принимать меры по предотвращению случаев разглашения (утечки) конфиденциальной информации и утраты документов, носителей информации; во взаимодействии с ОЗИ проводить постоянную работу по выявлению возможных каналов утечки информации и их закрытию, по совершенствованию системы защиты информации.

14 Определять порядок использования в подразделении работниками мобильных электронных устройств; перед проведением служебных совещаний, конференций, собраний, учебных занятий и других массовых мероприятий при необходимости требовать от присутствующих отключать средства мобильной связи и другие устройства.

15 Организовать и поддерживать систему парольной защиты информации в средствах вычислительной техники в соответствии с инструкцией (Приложение К).

16 Организовать резервное копирование и архивирование конфиденциальной и открытой ценной (важной) информации.

17 Согласовывать с ОЗИ проведение работ по созданию, модернизации и внедрению объектов информатизации, а также все проводимые мероприятия и принимаемые меры по защите информации.

18 В случае инцидента информационной безопасности (утечка конфиденциальной информации, несанкционированный доступ к информационным ресурсам, ИС и сервисам, несанкционированное воздействие на них, утеря конфиденциальных документов и носителей электронной информации, др.) информировать об этом ОЗИ и ДИТ, принимать меры по их пресечению.

19 Предоставлять сотрудникам ОЗИ затребованную информацию, в т.ч. конфиденциальную, беспрепятственно допускать их к объектам информатизации и информационным ресурсам подразделения в соответствии с их должностными обязанностями и полномочиями.

За нарушение требований настоящей инструкции руководитель подразделения несёт ответственность в соответствии с действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ Б

Инструкция по защите информации работнику СФУ

Работник обязан:

1 Знать и строго выполнять требования по эксплуатации технических средств, вверенных ему в пользование для служебных целей, нормативных документов по ведению делопроизводства, технологии обработки (передачи) и защиты информации.

2 Работать только с теми служебными документами и сведениями, а также техническими средствами, к которым он получил доступ в силу своих служебных обязанностей.

3 Не разглашать ставшую известной ему по службе и/или иным путём конфиденциальную информацию СФУ.

4 Обеспечить сохранность доверенных ему по службе документов, как на бумажной основе, так и машинных носителей информации (флэш-накопители, внешние накопители на жестких дисках, компакт-диски, иные устройства, фото-, кино-, видео- и аудиопленки, и др.), вести их учёт и хранение в установленном порядке.

5 Обеспечить сохранность ключевого носителя (электронного идентификатора), периодически менять на нем пароль, не передавать ключ другим лицам, не оставлять его без присмотра, в случае утраты ключа необходимо немедленно сообщить об этом администратору.

6 Соблюдать требования Инструкции по парольной защите при работе на средствах вычислительной техники (Приложение К).

7 Содержать на рабочем месте мониторы, печатающие устройства, а также конфиденциальные документы таким образом, чтобы исключить визуальный просмотр информации посторонними (посетителями).

8 Перед началом работы на ПЭВМ, в информационных системах и сервисах проверять наличие и работоспособность антивирусных программ, следить за их своевременным обновлением. Все электронные носители информации перед их применением проверять на наличие вирусов.

9 Оставляя рабочее место независимо от времени, активизировать временную блокировку экрана монитора и клавиатуры ПЭВМ.

10 Ставить в известность руководителя подразделения и сетевого администратора (администратора ИС) обо всех подозрительных ситуациях (нарушение функционирования средств вычислительной техники, ИС, изменение конфигурации программного обеспечения, наличие вируса и т. п.).

11 Передавать служебные документы, в т.ч. неконфиденциальные, только в соответствии с установленной информационной технологией и/или по распоряжению (указанию) руководителя подразделения. Конфиденциальные документы передавать только под подпись установленным порядком.

12 Служебный электронный документооборот, в т.ч. и неконфиденциальный, вести только посредством корпоративных ИС и сервисов, к которым работник допущен письменным приказом (распоряжением). Запрещается использовать для служебного документооборота, в т.ч. неконфиденциального, некорпоративные информационные системы и сервисы (электронная почта, мессенджеры, облачные технологии и др.).

13 По согласованию с руководителем подразделения установленным порядком создавать и хранить резервные копии конфиденциальной и открытой ценной (важной)

информации. Резервные копии хранить в местах, указанных руководителем подразделения и недоступных для других местах (запирающиеся сейфы, шкафы, др.).

14 Пресекать действия посторонних лиц (посетителей) и других работников, направленные на разглашение конфиденциальной информации, создание предпосылок к нарушению ее безопасности, а также на несанкционированный доступ к доверенной ему

служебной информации, требовать от них соблюдения установленного порядка в служебном помещении. В случае невыполнения этих требований сообщать своему руководителю или в службу безопасности.

15 Не выносить из служебного помещения конфиденциальные документы и другие носители конфиденциальной информации без разрешения (распоряжения) своего руководителя.

16 Не допускать без разрешения (распоряжения) своего руководителя к работе на технических средствах (вычислительная и оргтехника, средства связи и др.), а также к контрольно-техническим, ремонтно-строительным и другим работам в служебном помещении посторонних (посетителей, работников не своего подразделения).

17 Не оставлять в служебном помещении при выходе из него посторонних (посетителей) одних, а конфиденциальные документы и носители электронной информации – доступными для других работников и посторонних (посетителей).

18 Никому не передавать, не сообщать конфиденциальную информацию по телефону, факсу, электронной почте, посредством мессенджеров и облачных технологий.

19 Не устанавливать, не удалять, не копировать, не переименовывать программное обеспечение на технических средствах, доверенных ему для работы, без согласования с руководителем своего подразделения и системным администратором (специалистом департамента информационных технологий).

20 Не сообщать свои пароли и идентификаторы другим лицам, в случае необходимости с разрешения (указания) руководителя подразделения хранить их записанными только в местах, недоступных для других.

21 Использовать мобильные электронные устройства (ноутбук, блокнотный, планшетный, портативный компьютер, личный цифровой помощник (персональный цифровой секретарь), радиоприемники, радиопередатчики, средства аудио, фото, видеозаписи, средства мобильной связи и др.) в помещениях университета только с разрешения руководителя подразделения. Перед проведением массовых служебных мероприятий (совещания, конференции, собрания и т.п.) указанные средства отключать.

22 Не осуществлять действия, направленные на несанкционированный доступ в другие средства вычислительной техники, вычислительные и радиосети, воздействие на инфракрасные и другие электронные системы.

За нарушение требований настоящей инструкции работник несёт ответственность в соответствии с действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ В

Инструкция
по защите информации обучающемуся СФУ

Обучающийся (студент, аспирант, слушатель) на учебных занятиях, других мероприятиях, при нахождении в помещениях университета обязан:

1 Знать и строго выполнять требования по эксплуатации технических средств, вверенных ему в пользование, технологию обработки информации.

2 Работать только с теми техническими и программными средствами, к которым он получил доступ от руководителя занятий или мероприятия, никого не допускать к работе с этими средствами без разрешения руководителя.

3 Не устанавливать, не удалять, не копировать, не переименовывать, не перемещать программное обеспечение, информационные ресурсы без согласования с руководителем.

4 На учебных занятиях не использовать без разрешения руководителя средства вычислительной техники в целях, не связанных с учебным процессом (компьютерные игры, чаты, форумы, конференции, социальные сети, электронная почта и т.п.).

5 Посещать Интернет-ресурсы во время учебных занятий только с разрешения руководителя и только образовательной направленности. Сообщать руководителю о случайном попадании на ресурс, явно не соответствующий образовательной направленности и/или нарушающий законодательство РФ с указанием Интернет-адреса ресурса (URL), затем немедленно покинуть ресурс.

6 При нарушении функционирования средств вычислительной техники, изменении конфигурации программного обеспечения, появлении программных ошибок, сбоях оборудования, обнаружении вирусов и неисправностей немедленно поставить в известность об этом руководителя.

7 Не устранять самостоятельно неисправности в работе средств вычислительной техники и других технических средств. Не вносить изменения в аппаратную конфигурацию компьютера (перенос клавиатуры/мыши с одного компьютера на другой, переключение мониторов, присоединение или отсоединение кабелей, разъемов, проводов, розеток и т.п.).

8 Использовать мобильные электронные устройства (ноутбук, блокнотный, планшетный компьютер, портативный миникомпьютер, личный цифровой помощник (персональный цифровой секретарь), радиоприемник, средства аудио, фото, видеозаписи, средства мобильной связи и другие устройства) при проведении учебных занятий, конференций, собраний и других массовых мероприятий только с разрешения руководителя занятий или проводимого мероприятия.

9 Соблюдать правила работы в вычислительных сетях университета, в том числе беспроводных.

10 Не осуществлять действия, направленные на несанкционированный доступ в другие средства вычислительной техники, вычислительные и радиосети, воздействие на инфракрасные и другие электронные системы.

11 В случае привлечения обучающегося к мероприятиям и работам по обеспечению учебной, научной, служебной и другой деятельности университета он обязан знать и строго выполнять требования по защите информации, предъявляемые к работнику университета.

За нарушение требований настоящей инструкции обучающийся несёт ответственность в соответствии с действующим законодательством Российской Федерации.

ПРИЛОЖЕНИЕ Г

Форма журнала доведения до работников (обучающихся) документов по защите информации

ЖУРНАЛ
доведения до работников (обучающихся) документов по защите информации

_____
наименование подразделения

№ п/п	Название документа, его реквизиты (дата, номер)	Кто и когда ознакомлен с документом				Примечание
		Фамилия, инициалы	Должность	Подпись	Дата	

_____ _____ _____
должность руководителя подразделения подпись фамилия, инициалы

ПРИЛОЖЕНИЕ Д

Форма списка информационных ресурсов, содержащих конфиденциальную информацию СФУ, информационных систем и сервисов

Список информационных ресурсов,
содержащих конфиденциальную информацию СФУ,
информационных систем и сервисов

_____,
наименование подразделения

№ п/п	Наименование ресурса (дело, документ, база данных, ИС, сервис)	Индекс дела по номенклатуре дел	Количество дел, АРМ с доступом к БД ИС	Адрес нахождения ресурса, АРМ с доступом к БД ИС	Примечание

_____ _____ _____
должность руководителя подразделения подпись фамилия, инициалы

Начальник отдела защиты информации УВБ _____ _____
подпись фамилия, инициалы

Примечание. Список утверждается приказом (распоряжением) ректора, проректора или директора института (филиала).

ПРИЛОЖЕНИЕ Е

Форма списка работников, допущенных к работе с конфиденциальной информацией СФУ, информационными системами и сервисами

Список работников

_____,
наименование подразделения

допущенных к работе с конфиденциальной информацией СФУ, информационными системами и сервисами

№ п/п	Должность	Фамилия, инициалы	Ресурсы (информация, ИС, сервис), к которым допущен работник	Права доступа к ресурсам	Примечание

_____ _____ _____
должность руководителя подразделения подпись фамилия, инициалы

Начальник отдела защиты информации УВБ _____ _____
подпись фамилия, инициалы

Примечание. Список утверждается приказом (распоряжением) ректора, проректора или директора института (филиала).

ПРИЛОЖЕНИЕ Ж

Форма списка защищаемых помещений и ответственных за них

Список защищаемых помещений и ответственных за них

_____
(наименование подразделения)

№ п/п	Адрес помещения	Назначение помещения	Ответственный за помещение	Рабочий телефон	Примечание

_____ _____ _____
должность руководителя подразделения подпись фамилия, инициалы

Начальник отдела защиты информации УВБ _____ _____
подпись фамилия, инициалы

Примечание. Список утверждается приказом (распоряжением) ректора, проректора или директора института (филиала).

ПРИЛОЖЕНИЕ И

Форма технического паспорта на защищаемое помещение

Министерство науки и высшего образования РФ
Федеральное государственное автономное образовательное учреждение
высшего образования
«СИБИРСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

ТЕХНИЧЕСКИЙ ПАСПОРТ
на защищаемое помещение № ____

_____

Назначение помещения

_____

Наименование подразделения

_____	_____	_____
должность руководителя подразделения	подпись	фамилия, инициалы
_____	_____	_____
ответственный за помещение	подпись	фамилия, инициалы

Начальник ОЗИ УВБ _____ _____
подпись инициалы, фамилия

Красноярск 20____

Продолжение приложения И

Типовая инструкция
по обеспечению режима допуска и работы
в защищаемом помещении № _____

1 Ответственность за режим допуска и работы в защищаемом помещении (ЗП), за соблюдением требований по защите информации в нем несет ответственный за помещение – (должность, фамилия, инициалы). При убытии ответственного за ЗП в отпуск, командировку и т.п. руководитель подразделения назначает одного из работников подразделения следить за соблюдением настоящей инструкции.

2 В нерабочее время, а также при отсутствии работников, имеющих допуск в это защищаемое помещение, оно должно закрываться на ключ. Выдача ключей от помещения и электронного ключа охранно-пожарной сигнализации работникам осуществляется по списку, определенному руководителем подразделения. По окончании работ назначенный руководителем подразделения работник обязан закрыть помещение на ключ, установить на охранно-пожарную сигнализацию, сдать под охрану установленным порядком.

3 Установка технических средств, оборудования, мебели, ремонт и замена их, а также ремонт помещения, уборка в помещении, другие работы в нем должны проводиться только с разрешения (указания) руководителя подразделения и в присутствии работников, имеющих допуск в это помещение. Запрещается при выходе из помещения оставлять в нем посторонних (посетителей, лиц, не допущенных для работы в этом помещении) одних, а конфиденциальные документы и носители электронной информации – доступными.

4 Должны строго выполняться предписания на эксплуатацию средств связи, вычислительной техники, оргтехники, бытовых приборов и другого оборудования, установленного в помещении. Техника и оборудование должны использоваться только для служебных целей.

5 Мобильные электронные устройства (ноутбук, блокнотный, планшетный, портативный компьютер, радиоприемник, радиопередатчик, средства аудио, фото, видеозаписи и другие устройства) использовать в помещении только с разрешения руководителя подразделения. Средства мобильной связи при проведении совещаний, собраний и других массовых мероприятий отключать.

6 За эксплуатацию и правильное использование технических средств на АРМ, соблюдение при этом требований по защите информации несет ответственность пользователь этого АРМ, а технических средств коллективного пользования – ответственный за помещение (фамилия, инициалы).

7 Контроль за выполнением установленного режима допуска и работы в помещении, за соблюдением требований по защите информации осуществляют руководитель подразделения, ответственный за защиту информации подразделения, сотрудники отдела защиты информации УВБ, а также назначенные для этого комиссии и должностные лица.

8 Паспорт должен храниться непосредственно в защищаемом помещении. Ответственный за помещение обязан своевременно вносить в него необходимые изменения. С паспортом должны быть ознакомлены под подпись все работники, имеющие доступ в него.

Примечание: Инструкция составляется для каждого конкретного защищаемого помещения с учетом его особенностей: назначения, проводимых работ, оборудования техническими средствами, хранимой и обрабатываемой информации, посещаемости работниками (обучающимися) и т. д.

Продолжение приложения И

Список работников,
допущенных к вскрытию (закрытию)
защищаемого помещения № ____

№ п/п	Фамилия, имя, отчество	Должность	Дополнительные полномочия	Примечание
1.	Иванов Петр Иванович	Специалист	Ответственный за ЗП	

_____ _____ _____
должность руководителя подразделения подпись фамилия, инициалы

Примечания:
1 При лишении работника допуска в помещение (увольнение, перевод в другое подразделение и др.) в графе «Примечание» делается отметка о лишении допуска.
Например: «Уволен. Приказ СФУ от _____ № ____».
2 Новый работник заносится в список.
3 Записи заверяются подписью руководителя подразделения.

Окончание приложения И

Перечень технических средств,

установленных в помещении

№ п/п	Техническое средство	Учетный (инв., заводской) номер. Дата установки, дата удаления	Наличие доступа на АРМ к ИС и сервисам, обрабатываемая информации	Ответственный за эксплуатацию технического средства
1.	ЭВМ Pentium 133/24	Инв. № 457680 Установлен 2024г. Удален 2026 г	- БД ИС «1С:ЭДО» - БД сетевого ресурса «sgi$» - БД АИИС «Элдис» **Обработка КИ (ПДн, ДСП)**	Иванов А.А.

_____ _____ _____

должность руководителя подразделения подпись фамилия, инициалы

Примечания:

1 При удалении технического средства из помещения проставляется дата удаления в графе **«Дата установки, дата удаления».**

2 Новые установленные технические средства вносятся в перечень.

Список работников,
ознакомленных с техническим паспортом
на защищаемое помещение № ___

№ п/п	Фамилия, инициалы	Подпись	Дата ознакомления	Примечание

Примечание.

В список вносятся все работники, упомянутые в техническом паспорте.

О выбывших делается запись в графе «Примечание».

ПРИЛОЖЕНИЕ К

Инструкция по организации парольной защиты при работе на средствах вычислительной техники

1 Ответственность за организацию системы парольной защиты несут:

в подразделении – руководитель подразделения;

в информационной (автоматизированной) системе и сервисе – руководитель подразделения, сопровождающего эту систему, сервис;

на АРМ – пользователь СВТ, информационной системы и сервиса.

2 Личные пароли генерируются и распределяются централизованно либо выбираются пользователями информационной системы (ПЭВМ) самостоятельно с учетом следующих требований:

– пароль должен состоять не менее чем из восьми символов, а для административных учетных записей не менее десяти; большее количество символов повышает его надежность;

– пароль обязательно должен состоять из букв и цифр; использование букв в верхнем и нижнем регистрах и специальные символы (@, #, $, &, *, % и т.п.) повышают его надежность;

– пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, известные названия, словарные и жаргонные слова и т. п.), последовательности символов и знаков (123, abcd и т. п.), общепринятые сокращения (ЭВМ, АРМ, ЛВС и т. п.), аббревиатуры, клички домашних животных, номера автомобилей, телефонов и другие значимые сочетания букв и знаков, которые можно предположить, вычислить, основываясь на информации о пользователе;

– новый пароль пользователя не должен совпадать с именем учетной записи пользователя и с предыдущими паролями, должен отличаться от старого не менее чем в шести позициях.

3 Пароли пользователей на доступ к различным ресурсам (для входа в операционную систему ПЭВМ, информационную систему, базы данных, электронной почты и др.) должны быть различными.

4 При вводе пароля пользователю необходимо исключить произнесение его вслух, возможность его видеть посторонними лицами (другими работниками, посетителями).

5 Запрещается включать пароли в какой-либо автоматизированный процесс начала сеанса, например с использованием хранимых макрокоманд или функциональных клавиш.

6 Смена паролей должна проводиться регулярно, не реже одного раза в три месяца, а также в случае прекращения полномочий пользователя (увольнение, переход в другое подразделение и т. п.) или в случае компрометации пароля (если он стал известен другим лицам или есть подозрение об этом).

7 Срочная (внеплановая) полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход в другое подразделение и т. п.) администраторов информационной системы и других работников, которым по роду работы были предоставлены полномочия по управлению системой парольной защиты.

Окончание приложения К

8 Смена пароля производится самостоятельно каждым пользователем в соответствии с п. 2. настоящей Инструкции и/или в соответствии с указанием в системном баннере-предупреждении (при наличии технической возможности).

9 Временный пароль, заданный системным администратором при регистрации нового пользователя, следует изменить при первом входе в систему.

10 Пользователь обязан сохранять в тайне свой индивидуальный пароль, не сообщать его другим лицам и не регистрировать их в системе под своим паролем.

11 Запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, хранить их в местах, доступных для других.

12 При технологической необходимости использования имен и паролей работников (исполнителей) в их отсутствие (в случае возникновения нештатных ситуаций, форс-мажорных обстоятельств и т. п.) по решению руководителя подразделения записанные пароли в запечатанном конверте могут храниться у руководителя подразделения или у другого назначенного им лица. Конверт с паролем должен храниться в защищаемом помещении в месте (сейф, надежно запирающийся шкаф и др.), исключающем несанкционированный доступ. В случае отсутствия пользователя при необходимости конверт с паролем может быть вскрыт руководителем подразделения или назначенным им лицом, факт вскрытия фиксируется служебной запиской, составлением акта или другим письменным документом. После экстренного вскрытия пароль должен быть изменен.

13 В информационных (автоматизированных) системах, обрабатывающих конфиденциальную информацию, необходимо использовать повышенные требования к парольной защите: автоматическую блокировку учетных записей пользователя в случае окончания срока действия пароля, после 3-5 неудачных попыток авторизации и в других случаях. При этом блокировка должна сниматься «вручную» системным администратором или специалистом службы технической поддержки с одновременной сменой пароля пользователя. В журнал системных событий сервера должно заноситься сообщение о многократно неудавшихся попытках авторизации пользователя.