МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное автономное образовательное учреждение высшего профессионального образования «Казанский (Приволжский) федеральный университет»

УТВЕРЖДАЮ
Ректор
И.Р. Гафуров
«___» _____ 20__ г.

КОНЦЕПЦИЯ
информационной безопасности инфокоммуникационных автоматизированных систем федерального государственного автономного образовательного учреждения высшего профессионального образования «Казанский (Приволжский) федеральный университет»

г. Казань – 2012

СОДЕРЖАНИЕ

ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АВС – антивирусные средства
АРМ – автоматизированное рабочее место
ВТСС – вспомогательные технические средства и системы
ИАС – инфокоммуникационная автоматизированная система
КЗ – контролируемая зона
КФУ – Казанский федеральный университет
ЛВС – локальная вычислительная сеть
МЭ – межсетевой экран
НСД – несанкционированный доступ
ОС – операционная система
ПМВ – программно-математическое воздействие
ПО – программное обеспечение
ПЭМИН – побочные электромагнитные излучения и наводки
САЗ – система анализа защищенности
СЗИ – система (средства) защиты информации
СОВ – система обнаружения вторжений
ТКУИ – технические каналы утечки информации
ТС – технические средства

ОПРЕДЕЛЕНИЯ

В настоящем документе используются следующие термины и их определения.

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Аутентификация отправителя данных – подтверждение того, что отправитель полученных данных соответствует заявленному.

Безопасность информации – состояние защищенности информации, характеризуемое способностью пользователей, технических средств и информационных технологий обеспечить конфиденциальность, целостность и доступность информации при её обработке в инфокоммуникационных автоматизированных системах (ИАС).

Биометрические персональные данные – сведения, которые характеризуют физиологические особенности человека и на основе которых можно установить его личность, включая фотографии, отпечатки пальцев, образ сетчатки глаза, особенности строения тела и другую подобную информацию.

Блокирование информации – временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе её передачи.

Вирус (компьютерный, программный) – исполняемый программный код или интерпретируемый набор инструкций, обладающий свойствами несанкционированного распространения и самовоспроизведения. Созданные дубликаты компьютерного вируса не всегда совпадают с оригиналом, но сохраняют способность к дальнейшему распространению и самовоспроизведению.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на персональные данные или ресурсы информационной системы персональных данных.

Доступ в операционную среду компьютера (информационной системы) – получение возможности запуска на выполнение штатных команд, функций, процедур операционной системы (уничтожения, копирования, перемещения и т.п.), исполняемых файлов прикладных программ.

Доступ к информации – возможность получения информации и ее использования.

Закладочное устройство – элемент средства съема информации, скрытно внедряемый (закладываемый или вносимый) в места возможного съема информации (в том числе в ограждение, конструкцию, оборудование, предметы интерьера, транспортные средства, а также в технические средства и системы обработки информации).

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информативный сигнал – электрические сигналы, акустические, электромагнитные и другие физические поля, по параметрам которых может быть раскрыта конфиденциальная информация, обрабатываемая в ИАС.

Инфокоммуникационная автоматизированная система – информационная система, представляющая собой совокупность конфиденциальной информации, содержащейся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

Источник угрозы безопасности информации – субъект доступа, материальный объект или физическое явление, являющиеся причиной возникновения угрозы безопасности информации.

Контролируемая зона – пространство (территория, здание, часть здания, помещение), в котором исключено неконтролируемое пребывание посторонних лиц, а также транспортных, технических и иных материальных средств.

Конфиденциальность информации – обязательное для соблюдения оператором или иным получившим доступ к защищаемой информации лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания.

Межсетевой экран – локальное (однокомпонентное) или функционально-распределенное программное (программно - аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в ИАС и (или) выходящей из ИАС.

Нарушитель безопасности персональных данных – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности защищаемой информации при их обработке техническими средствами в ИАС.

Недекларированные возможности – функциональные возможности средств вычислительной техники, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых информационными системами персональных данных.

Носитель информации – физическое лицо или материальный объект (например, «флэш» – носитель), в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обезличивание персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных.

Перехват (информации) – неправомерное получение информации с использованием технического средства, осуществляющего обнаружение, прием и обработку информативных сигналов.

Побочные электромагнитные излучения и наводки – электромагнитные излучения технических средств обработки защищаемой информации, возникающие как побочное явление и вызванные электрическими сигналами, действующими в их электрических и магнитных цепях, а также электромагнитные наводки этих сигналов на токопроводящие линии, конструкции и цепи питания.

Пользователь ИАС – лицо, участвующее в функционировании информационной системы или использующее результаты ее функционирования.

Правила разграничения доступа – совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Программная закладка – код программы, преднамеренно внесенный в программу с целью осуществить утечку, изменить, блокировать, уничтожить информацию или уничтожить и модифицировать программное обеспечение информационной системы и (или) блокировать аппаратные средства.

Программное (программно-математическое) воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Ресурс информационной системы – именованный элемент системного, прикладного или аппаратного обеспечения функционирования информационной системы.

Средства вычислительной техники – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Субъект доступа (субъект) – лицо или процесс, действия которого регламентируются правилами разграничения доступа.

Технический канал утечки информации – совокупность носителя информации (средства обработки), физической среды распространения информативного сигнала и средств, которыми добывается защищаемая информация.

Технические средства ИАС – средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации (средства и системы звукозаписи, звукоусиления, звуковоспроизведения, переговорные и телевизионные устройства, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео и буквенно-цифровой информации), программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

Угрозы безопасности ИАС– совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к защищаемой информации, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение информации, а также иных несанкционированных действий при их обработке в ИАС.

Уничтожение информации – действия, в результате которых невозможно восстановить содержание информации в ИАС или в результате которых уничтожаются материальные носители персональных данных.

Университет – Казанский (Приволжский) федеральный университет.

Утечка (защищаемой) информации по техническим каналам – неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации.

Уязвимость – слабость в средствах защиты, которую можно использовать для нарушения системы или содержащейся в ней информации.

Целостность информации – способность средства вычислительной техники или автоматизированной системы обеспечивать неизменность информации в условиях случайного и/или преднамеренного искажения (разрушения).

1. Общие положения

1.1.Настоящая Концепция информационной безопасности инфокоммуникационных автоматизированных систем федерального государственного автономного образовательного учреждения высшего профессионального образования «Казанский (Приволжский) федеральный университет» разработана Управлением кадров КФУ, является официальным документом, в котором определена система взглядов на обеспечение информационной безопасности в КФУ.

Необходимость разработки Концепции обусловлена стремительным расширением сферы применения новейших информационных технологий и процессов в Университете при обработке конфиденциальной информации, в том числе персональных данных.

Концепция определяет основные цели, задачи, общую стратегию построения системы защиты информации (СЗИ) в ИАС КФУ, а также базовые подходы к их реализации, для достижения требуемого уровня безопасности информации.

Правовой базой для разработки настоящей Концепции служат требования действующих в Российской Федерации законодательных и нормативных актов по обеспечению безопасности информации.

1.2. СЗИ в КФУ представляет собой совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа к ней, уничтожения, изменения, блокирования, копирования, распространения.

1.3. Структура, состав и основные функции СЗИ определяются исходя из класса ИАС. СЗИ включает организационные меры и технические средства защиты информации (в том числе шифровальные (криптографические) средства), средства предотвращения несанкционированного доступа, средства защиты от утечки информации по техническим каналам, средства защиты от программно-технических воздействий на технические средства обработки информации, а также на используемые в информационной системе информационные технологии.

1.4. Организационные меры и технические средства защиты призваны обеспечить:

– конфиденциальность информации (защита от несанкционированного ознакомления);

– целостность информации (актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения);

– доступность информации (возможность за приемлемое время получить требуемую информационную услугу).

1.5. Процедура создания СЗИ как правило включает следующие стадии:

– предпроектная стадия, включающая в себя обследование ИАС и разработку технического задания на ее создание;

– стадия проектирования, включающая разработку СЗИ в составе ИАС;

– стадия ввода в эксплуатацию СЗИ, включающая опытную эксплуатацию и приемосдаточные испытания, а также оценку соответствия ИАС требованиям безопасности информации.

1.6. Организационные меры предусматривают создание и поддержание правовой базы безопасности информации в актуальном состоянии, разработку и введение в действие предусмотренных «Политикой информационной безопасности КФУ» следующих организационно-распорядительных документов:

1) План мероприятий по обеспечению защиты информации при ее обработке в ИАС;

2) План мероприятий по контролю обеспечения защиты информации;

3) Порядок резервирования и восстановления работоспособности ТС и ПО, баз данных и СЗИ;

4) Инструкция администратора ИАС в части обеспечения безопасности информации при их обработке;

5) Инструкция администратора безопасности ИАС;

6) Инструкция пользователя ИАС в части обеспечения безопасности информации при ее обработке в ИАС;

7) Инструкция пользователя на случай возникновения внештатной ситуации.

1.7. Технические меры защиты реализуются при помощи соответствующих программно-технических средств и методов защиты. Перечень необходимых мер защиты информации определяется по результатам внутренней проверки безопасности ИАС КФУ.

2. Основные задачи ИАС КФУ

2.1. Основными задачами ИАС КФУ являются:

2.1.1. Создание эффективной системы управления Университетом за счет информационно-аналитического обеспечения и интеграции информационных ресурсов.

2.1.2. Предоставление возможности быстрого доступа к данным по важнейшим показателям развития КФУ за любой период времени.

2.1.3. Представление данных в удобном для восприятия и анализа виде.

2.1.4. Получение возможности выявлять и прогнозировать тенденции развития социально-экономических процессов на всех уровнях управления КФУ.

2.1.5. Повышение эффективности и скорости принятия управленческих решений за счет использования новых возможностей, предоставляемых ИАС.

2.1.6. Уменьшение числа информационных посредников за счет использования передовых информационных технологий.

2.1.7. Сокращение бумажного оборота документов и отчетов при внедрении электронного документооборота.

2.1.8. Обеспечение информационной безопасности ИАС КФУ.

3. Управление ИАС КФУ

3.1. Обеспечение технического функционирования ИАС КФУ осуществляется Департаментом информатизации и связи КФУ.

3.2. Программно-техническое сопровождение ИАС КФУ, разработка новых программных модулей и обеспечение сохранности информации на серверах ИАС КФУ осуществляются отделами Департамента информатизации и связи или компаниями, привлекаемыми на конкурсной основе.

3.3. Для управления процессом внедрения ИАС КФУ приказом ректора утверждается рабочая группа, либо назначается ответственное лицо из числа сотрудников КФУ.

4. Цель СЗИ

4.1. Основной целью СЗИ является минимизация ущерба от возможной реализации угроз безопасности информации.

5. Задачи СЗИ ИАС

5.1. Для достижения основной цели система безопасности информационных ресурсов ИАС должна обеспечивать эффективное решение следующих задач:

5.1.1. Защиту от вмешательства в процесс функционирования ИАС посторонних лиц (возможность использования ИАС и доступ к ее ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

5.1.2. Разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИАС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИАС для выполнения своих служебных обязанностей), то есть защиту от несанкционированного доступа:

а) к информации, циркулирующей в ИАС;

б) средствам вычислительной техники ИАС;

в) аппаратным, программным и криптографическим средствам защиты, используемым в ИАС.

5.1.3. Регистрацию действий пользователей при использовании защищаемых ресурсов ИАС в системных журналах и периодический контроль корректности действий пользователей путем анализа содержимого этих журналов;

5.1.4. Контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;

5.1.5. Защиту от несанкционированной модификации и контроль целостности используемых в ИАС программных средств, а также защиту системы от внедрения несанкционированных программ;

5.1.6. Защиту информации от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;

5.1.7. Защиту информации, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

5.1.8. Обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

5.1.9. Своевременное выявление источников угроз безопасности информации, создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;

5.1.10. Создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации

6. Объекты защиты

6.1 В КФУ производится обработка конфиденциальной информации в том числе, персональных данных в следующих информационных системах:

ИАС “Абитуриент”;
ИАС “Аспирантура”;
ИАС “Иностранный гражданин”;
ИАС “Сотрудник”;
ИАС “Студент”;
ИАС “Электронный университет. Документооборот”;
АБИС “Руслан”;
ПП “Парус”;
ПП “1С Бухгалтерия”
ПП “1С Зарплата и кадры”;
ПП “Налогоплательщик”;
ПП “Коммунальные платежи”;
ПП “ПУ-5 (Персонифицированный учет)”;
ПП “Управление кадров”;
ПП “CheckXML”;
ПП “FilePfrXML”;
ПП “eDo”;
ПП “PARSEC”;
ПП “PERCO”.

6.2 Перечень информационных ресурсов, подлежащих защите, определяется нормативными правовыми документами регуляторов РФ и приказом ректора КФУ.

Объектами защиты ИАС КФУ являются:

1) Обрабатываемая информация.
2) Технологическая информация.

3) Программно-технические средства обработки.
4) Средства защиты информации.
5) Каналы информационного обмена и телекоммуникации.
6) Объекты и помещения, в которых размещены компоненты ИАС.

7. Классификация пользователей ИАС КФУ

7.1. Пользователем ИАС является лицо, участвующее в функционировании ИАС КФУ или использующее результаты ее функционирования.

Пользователем ИАС является любой работник или обучающийся КФУ, имеющий доступ к ИАС и ее ресурсам в соответствии с установленным порядком и функциональными обязанностями.

7.2. Пользователи ИАС делятся на три основные категории:

Администратор сети ИАС.

Сотрудники КФУ, которые занимаются настройкой, внедрением и сопровождением системы. Администратор ИАС обладает следующим уровнем доступа:

– обладает полной информацией о системном и прикладном программном обеспечении ИАС;

– обладает полной информацией о технических средствах и конфигурации ИАС;

– имеет доступ ко всем техническим средствам обработки информации и данным ИАС;

– имеет доступ к СЗИ;

– обладает правами конфигурирования и административной настройки технических средств ИАС.

Программист-разработчик ИАС (Администратор баз данных).

Сотрудники КФУ или сторонних организаций, которые занимаются разработкой программного обеспечения. Разработчик ИАС обладает следующим уровнем доступа:

– обладает информацией об алгоритмах и программах обработки информации на ИАС;

– обладает возможностями устранения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в программное обеспечение ИАС на стадии ее разработки, внедрения и сопровождения;

– может располагать любыми фрагментами информации о топологии ИАС и технических средствах обработки и защиты информации, обрабатываемых в ИАС.

Оператор ИАС.

Сотрудники подразделений КФУ, участвующие в процессе эксплуатации ИАС. Оператор ИАС обладает следующим уровнем доступа:

– обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству информационных ресурсов;

– располагает конфиденциальными данными, к которым имеет доступ.

7.3. Категории пользователей должны быть определены для каждой подсистемы ИАС. Должно быть уточнено разделение сотрудников внутри категорий, в соответствии с типами пользователей определенными в «Политике информационной безопасности КФУ».

7.4. Все выявленные группы пользователей отражаются в «Отчете по результатам внутренней проверки». На основании Отчета определяются права доступа к элементам ИАС для всех групп пользователей и отражаются в матрице доступа в «Положении о разграничении прав доступа к обрабатываемой информации ограниченного доступа».

8. Основные принципы построения системы комплексной защиты информации

Построение системы обеспечения безопасности информации ИАС КФУ и ее функционирование должны осуществляться в соответствии со следующими основными принципами:

– законность;

– системность;

– комплексность;
– непрерывность;
– своевременность;
– преемственность и непрерывность совершенствования;
– персональная ответственность;
– минимизация полномочий;
– взаимодействие и сотрудничество;
– гибкость системы защиты;
– открытость алгоритмов и механизмов защиты;
– простота применения средств защиты;
– научная обоснованность и техническая реализуемость;
– специализация и профессионализм;
– обязательность контроля.

8.1. Законность.

Предполагает осуществление защитных мероприятий и разработку СЗИ КФУ в соответствии с действующим законодательством в области защиты информации и других нормативных актов по безопасности информации, утвержденных органами государственной власти и управления в пределах их компетенции.

Пользователи и персонал обслуживающие (обрабатывающие) информацию ограниченного доступа ИАС КФУ должны быть осведомлены о порядке работы с защищаемой информацией и о персональной ответственности за утечку защищаемой информации.

8.2. Системность.

Системный подход к построению СЗИ КФУ предполагает учет всех взаимосвязанных, взаимодействующих и изменяющихся во времени элементов, условий и факторов, существенно-значимых для понимания и решения проблемы обеспечения безопасности информации, обрабатываемой в ИАС КФУ.

При создании системы защиты должны учитываться все слабые и наиболее уязвимые места системы обработки защищаемой информации, а также характер, возможные объекты и направления атак на систему со стороны нарушителей (особенно высококвалифицированных злоумышленников), пути проникновения в распределенные системы и НСД к информации. Система защиты должна строиться с учетом не только всех известных каналов проникновения и НСД к информации, но и с учетом возможности появления принципиально новых путей реализации угроз безопасности.

8.3. Комплексность.

Комплексное использование методов и средств защиты предполагает согласованное применение разнородных средств, при построении целостной системы защиты, перекрывающей все существенные (значимые) каналы реализации угроз и не содержащей слабых мест на стыках отдельных ее компонентов.

Защита должна строиться эшелонировано. Для каждого канала утечки информации и для каждой угрозы безопасности должно существовать несколько защитных рубежей. Создание защитных рубежей осуществляется с учетом того, чтобы для их преодоления потенциальному злоумышленнику требовались профессиональные навыки в нескольких невзаимосвязанных областях.

Внешняя защита должна обеспечиваться физическими средствами, организационными и правовыми мерами. Одним из наиболее укрепленных рубежей призваны быть средства криптографической защиты, реализованные с использованием технологии VPN. Прикладной уровень защиты, учитывающий особенности предметной области, представляет внутренний рубеж защиты.

8.4. Непрерывность защиты ИАС.

Защита ИАС – не разовое мероприятие и не простая совокупность проведенных мероприятий и установленных средств защиты, а непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла ИАС.

ИАС должна находиться в защищенном состоянии на протяжении всего времени её функционирования. В соответствии с этим принципом должны приниматься меры по недопущению перехода ИАС в незащищенное состояние.

Большинству физических и технических средств защиты для эффективного выполнения своих функций необходима постоянная техническая и организационная (административная) поддержка (своевременная смена и обеспечение правильного хранения и применения имен, паролей, ключей шифрования, перераспределение полномочий и т.п.). Перерывы в работе средств защиты могут быть использованы злоумышленниками для анализа применяемых методов и средств защиты, для внедрения специальных программных и аппаратных «закладок» и других средств преодоления системы защиты после восстановления ее функционирования.

8.5.Своевременность.

Предполагает упреждающий характер мер обеспечения безопасности информации, то есть постановку задач по комплексной защите ИАС и реализацию мер обеспечения безопасности информации на ранних стадиях разработки ИАС в целом и ее системы защиты информации, в частности.

Разработка системы защиты должна вестись параллельно с разработкой и развитием самой защищаемой системы. Это позволит учесть требования безопасности при проектировании архитектуры и, в конечном счете, создать более эффективные (как по затратам ресурсов, так и по стойкости) защищенные системы.

8.6. Преемственность и совершенствование.

Предполагают постоянное совершенствование мер и средств защиты информации на основе преемственности организационных и технических решений, кадрового состава, анализа функционирования ИАС и ее системы защиты с учетом изменений в методах и средствах перехвата информации, нормативных требований по защите, достигнутого отечественного и зарубежного опыта в этой области.

8.7. Персональная ответственность.

Предполагает возложение ответственности за обеспечение безопасности информации и системы их обработки на каждого сотрудника в пределах его полномочий. В соответствии с этим принципом распределение прав и обязанностей сотрудников строится таким образом, чтобы в случае любого нарушения круг виновников был четко известен или сведен к минимуму.

8.8. Принцип минимизации полномочий.

Означает предоставление пользователям минимальных прав доступа в соответствии с производственной необходимостью, на основе принципа «все, что не разрешено, запрещено».

Доступ к информации должен предоставляться только в том случае и объеме, если это необходимо сотруднику для выполнения его должностных обязанностей.

8.9. Взаимодействие и сотрудничество.

Предполагает создание благоприятной атмосферы в коллективах подразделений, обеспечивающих деятельность ИАС КФУ, для снижения вероятности возникновения негативных действий связанных с человеческим фактором.

В такой обстановке сотрудники должны осознанно соблюдать установленные правила и оказывать содействие в деятельности подразделений технической защиты информации.

8.10. Гибкость системы защиты конфиденциальной информации.

Принятые меры и установленные средства защиты, особенно в начальный период их эксплуатации, могут обеспечивать как чрезмерный, так и недостаточный уровень защиты. Для обеспечения возможности варьирования уровнем защищенности, средства защиты должны обладать определенной гибкостью. Особенно важным это свойство является в тех случаях, когда установку средств защиты необходимо осуществлять на работающую систему, не нарушая процесса ее нормального функционирования.

8.11. Открытость алгоритмов и механизмов защиты.

Суть принципа открытости алгоритмов и механизмов защиты состоит в том, что защита не должна обеспечиваться только за счет секретности структурной организации и алгоритмов функционирования ее подсистем. Знание алгоритмов работы системы защиты не должно давать возможности ее преодоления (даже авторам). Однако это не означает, что информация о конкретной системе защиты должна быть общедоступна.

8.12. Простота применения средств защиты.

Механизмы защиты должны быть интуитивно понятны и просты в использовании. Применение средств защиты не должно быть связано со знанием специальных языков или с выполнением действий, требующих значительных дополнительных трудозатрат при обычной работе зарегистрированных установленным порядком пользователей, а также не должно требовать от пользователя выполнения рутинных малопонятных ему операций (ввод нескольких паролей и имен и т.д.).

Должна достигаться автоматизация максимального числа действий пользователей и администраторов ИАС.

8.13. Научная обоснованность и техническая реализуемость.

Информационные технологии, технические и программные средства, средства и меры защиты информации должны быть реализованы на современном уровне развития науки и техники, научно обоснованы с точки зрения достижения заданного уровня безопасности информации, и должны соответствовать установленным нормам и требованиям по безопасности информации.

СЗИ должна быть ориентирована на решения, возможные риски для которых меры противодействия этим рискам прошли всестороннюю теоретическую и практическую проверку.

8.14. Специализация и профессионализм.

Предполагает привлечение к разработке средств и реализации мер защиты информации специализированных организаций, наиболее подготовленных к конкретному виду деятельности по обеспечению безопасности информации, имеющих опыт практической работы и государственную лицензию на право оказания услуг в этой области. Реализация административных мер и эксплуатация средств защиты должна осуществляться профессионально подготовленными специалистами КФУ.

8.15. Обязательность контроля.

Предполагает обязательность и своевременность выявления и пресечения попыток нарушения установленных правил обеспечения безопасности конфиденциальной информации, на основе используемых систем и средств защиты информации при совершенствовании критериев и методов оценки эффективности этих систем и средств.

Контроль за деятельностью любого пользователя, каждого средства защиты и в отношении любого объекта защиты должен осуществляться на основе применения средств оперативного контроля и регистрации и должен охватывать как несанкционированные, так и санкционированные действия пользователей.

9. Меры, методы и средства обеспечения требуемого уровня защищенности

Обеспечение требуемого уровня защищенности должен достигаться с использованием мер, методов и средств безопасности. Все меры обеспечения безопасности защищаемой информации подразделяются на:

– законодательные (правовые);
– морально-этические;
– организационные (административные);
– физические;
– технические (аппаратные и программные).

9.1. Перечень выбранных мер обеспечения безопасности отражается в «Плане мероприятий по обеспечению защиты информации».

9.2. Законодательные (правовые) меры защиты.

К правовым мерам защиты относятся действующие в стране законы, указы и нормативные акты, регламентирующие правила обращения с защищаемой информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил, препятствуя тем самым неправомерному использованию информации и являющиеся сдерживающим фактором для потенциальных нарушителей.

Правовые меры защиты носят в основном упреждающий, профилактический характер и требуют постоянной разъяснительной работы с пользователями и обслуживающим персоналом системы.

9.3. Морально-этические меры защиты.

9.3.1. К морально-этическим мерам относятся нормы поведения, которые традиционно сложились или складываются по мере распространения ИАС в стране или обществе. Эти нормы большей частью не являются обязательными, как законодательно утвержденные нормативные акты, однако, их несоблюдение ведет обычно к падению авторитета, престижа человека, группы лиц или организации. Морально-этические нормы бывают как неписаные (например, общепризнанные нормы честности, патриотизма и т.п.), так и писаные, то есть оформленные в некоторый свод (устав) правил или предписаний.

9.3.2. Морально-этические меры защиты являются профилактическими и требуют постоянной работы по созданию здорового морального климата в коллективах подразделений КФУ. Морально-этические меры защиты снижают вероятность возникновения негативных действий связанных с человеческим фактором.

9.4. Организационные (административные) меры защиты.

9.4.1. Организационные (административные) меры защиты – это меры организационного характера, регламентирующие процессы функционирования ИАС, использование ресурсов ИАС, деятельность обслуживающего персонала, а также порядок взаимодействия пользователей с ИАС таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности или снизить размер потерь в случае их реализации.

9.4.2. Главная цель административных мер, предпринимаемых на высшем управленческом уровне – сформировать «Политику информационной безопасности ИАС» (отражающую подходы к защите информации) и обеспечить ее выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

9.4.3. Реализация «Политики информационной безопасности ИАС» в ИАС состоит из мер административного уровня и организационных (процедурных) мер защиты информации.

9.4.4. К административному уровню относятся решения руководства, затрагивающие деятельность ИАС в целом. Эти решения закрепляются в политике информационной безопасности. Примером таких решений могут быть:

– принятие решения о формировании или пересмотре комплексной программы обеспечения безопасности ИАС, определение ответственных за ее реализацию;

– формулирование целей, постановка задач, определение направлений деятельности в области безопасности ИАС;

– принятие решений по вопросам реализации программы безопасности, которые рассматриваются на уровне КФУ в целом;

– обеспечение нормативной (правовой) базы вопросов безопасности и т.п.

9.4.5. Политика верхнего уровня должна четко очертить сферу влияния и ограничения при определении целей безопасности информации, определить какими ресурсами (материальные, персонал) они будут достигнуты и найти разумный компромисс между приемлемым уровнем безопасности и функциональностью ИАС.

9.4.6. На организационном уровне определяются процедуры и правила достижения целей и решения задач «Политики информационной безопасности ИАС». Эти правила определяют:

– какова область применения политики безопасности ИАС;

– каковы роли и обязанности должностных лиц, отвечающих за проведение политики безопасности ИАС, а так же их ответственность;

– кто имеет права доступа к защищаемой информации;

– какими мерами и средствами обеспечивается защита информации по требованиям безопасности;

– какими мерами и средствами обеспечивается контроль за соблюдением введенного режима безопасности.

9.4.7. Организационные меры должны:

– предусматривать регламент информационных отношений, исключающих возможность несанкционированных действий в отношении объектов защиты;

– определять коалиционные и иерархические принципы и методы разграничения доступа к ПДн;

– определять порядок работы с программно-математическими и техническими (аппаратные) средствами защиты и криптозащиты и других защитных механизмов;

– определять меры противодействия НСД пользователями на этапах аутентификации, авторизации, идентификации, обеспечивающие гарантии реализации прав и ответственности субъектов информационных отношений.

9.4.8. Организационные меры должны состоять из:

– регламента доступа в помещения, в которых расположены серверы ИАС;

– порядок допуска сотрудников к использованию ресурсов ИАС КФУ;

– регламента процессов ведения баз данных и осуществления модификации информационных ресурсов;

– регламента процессов обслуживания и осуществления модификации аппаратных и программных ресурсов ИАС;

– инструкций пользователей ИАС (администратора ИАС, администратора безопасности, оператора ИАС);

– инструкция пользователя при возникновении внештатных ситуаций.

9.5. Физические меры защиты.

9.5.1. Физические меры защиты основаны на применении разного рода механических, электро- или электронно-механических устройств и сооружений, специально предназначенных для создания физических препятствий на возможных путях проникновения и доступа потенциальных нарушителей к компонентам системы и защищаемой информации, а также технических средств визуального наблюдения, связи и охранной сигнализации.

9.5.2. Физическая защита зданий, помещений, объектов и средств информатизации должна осуществляться путем установления соответствующих постов охраны, с помощью технических средств охраны или любыми другими способами, предотвращающими или существенно затрудняющими проникновение в здание, помещения посторонних лиц, хищение информационных носителей, самих средств информатизации, исключающими нахождение внутри контролируемой (охраняемой) зоны технических средств разведки.

9.6. Аппаратно-программные средства защиты информации

9.6.1. Технические (аппаратно-программные) меры защиты основаны на использовании различных электронных устройств и специальных программ, входящих в состав ИАС и выполняющих (самостоятельно или в комплексе с другими средствами) функции защиты (идентификацию и аутентификацию пользователей, разграничение доступа к ресурсам, регистрацию событий, криптографическое закрытие информации и т.д.).

9.6.2. С учетом всех требований и принципов обеспечения безопасности информации в ИАС по всем направлениям защиты в состав системы защиты должны быть включены следующие средства:

– средства идентификации (опознавания) и аутентификации (подтверждения подлинности) пользователей ИАС;

– средства разграничения доступа зарегистрированных пользователей системы к ресурсам ИАС КФУ;

– средства обеспечения и контроля целостности программных и информационных ресурсов;

– средства оперативного контроля и регистрации событий безопасности;

– криптографические средства защиты информации.

9.6.3. Успешное применение технических средств защиты предполагает, что выполнение перечисленных ниже требований обеспечено организационными (административными) мерами и используемыми физическими средствами защиты:

– обеспечена физическая целостность всех компонентов ИАС;

– каждый сотрудник (пользователь ИАС) или группа пользователей имеет уникальное системное имя и минимально необходимые для выполнения им своих функциональных обязанностей полномочия по доступу к ресурсам системы;

– в ИАС КФУ разработка и отладка программ осуществляется за пределами ИАС, на испытательных стендах;

– все изменения конфигурации технических и программных средств ИАС производятся строго установленным порядком (регистрируются и контролируются) только на основании распоряжений руководства Департамента информатизации и связи КФУ;

– сетевое оборудование (концентраторы, коммутаторы, маршрутизаторы и т.п.) располагается в местах, недоступных для посторонних (специальных помещениях, шкафах, и т.п.).

– специалистами КФУ осуществляется непрерывное управление и административная поддержка функционирования средств защиты.

10. Контроль эффективности системы защиты ИАС КФУ

10.1. Контроль эффективности СЗИ должен осуществляется на периодической основе. Целью контроля эффективности является своевременное выявление ненадлежащих режимов работы СЗИ (отключение средств защиты, нарушение режимов защиты, несанкционированное изменение режима защиты и т.п.), а также прогнозирование и превентивное реагирование на новые угрозы безопасности информации.

10.2. Контроль может проводиться как администраторами информационной безопасности ИАС (оперативный контроль в процессе информационного взаимодействия в ИАС), так и привлекаемыми для этой цели компетентными организациями, имеющими лицензию на этот вид деятельности, а также ФСТЭК России и ФСБ России в пределах их компетенции.

10.3. Контроль может осуществляться администратором информационной безопасности как с помощью штатных средств системы защиты информации, так и с помощью специальных программных средств контроля.

10.4. Оценка эффективности мер защиты проводится с использованием технических и программных средств контроля на предмет соответствия установленным требованиям.

11. Сферы ответственности за безопасность информации

11.1. Ответственным за разработку мер и контроль над обеспечением безопасности персональных данных является начальник Управления кадров КФУ.

11.2. Ответственным за разработку мер и контроль над обеспечением информационной безопасности является начальник Департамента информатизации и связи КФУ.

11.3. Сфера ответственности лиц, ответственных за обеспечение безопасности информации, включает следующие направления:

– планирование и реализацию мер по обеспечению безопасности защищаемой информации;

– анализ угроз безопасности защищаемой информации;

– разработку, внедрение, контроль исполнения и поддержание в актуальном состоянии политик, руководств, концепций, процедур, регламентов, инструкций и других организационных документов по обеспечению безопасности информации;

– контроль защищенности информационно-технической инфраструктуры КФУ от угроз осуществляется путем обучения и информирования пользователей ИАС о порядке работы с защищаемой информацией и средствами защиты, предотвращением, выявлением, реагированием и расследованием нарушений безопасности ИАС.

11.4. При взаимодействии со сторонними организациями в случаях, когда сотрудникам этих организаций предоставляется доступ к объектам защиты, с этими организациями должно быть заключено «Соглашение о конфиденциальности», либо «Соглашение о соблюдении режима безопасности защищаемой информации при выполнении работ в ИАС». Подготовка типовых вариантов этих соглашений осуществляется совместно с юридическим управлением.

12. Модель нарушителя безопасности

12.1. Под нарушителем понимается лицо, которое в результате умышленных или неумышленных действий может нанести ущерб объектам защиты.

12.2. Нарушители подразделяются по признаку принадлежности к ИАС. Все нарушители делятся на две группы:

• внешние нарушители – физические лица, не имеющие права пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИАС КФУ;

• внутренние нарушители – физические лица, имеющие право пребывания на территории контролируемой зоны, в пределах которой размещается оборудование ИАС КФУ.

12.3. Классификация нарушителей должна быть представлена в «Модели угроз безопасности ИАС КФУ» или в «Модели угроз безопасности персональных данных при их обработке в информационных системах персональных данных».

13. Модель угроз безопасности

13.1. Для ИАС КФУ выделяются следующие основные категории угроз безопасности защищаемой информации:

– Угрозы от утечки по техническим каналам.

– Угрозы несанкционированного доступа к информации.

13.2. Описание угроз, вероятность их реализации, опасность и актуальность должна быть представлена в «Модели угроз безопасности ИАС КФУ».

14. Механизм реализации Концепции

14.1. Реализация Концепции должна осуществляться на основе перспективных программ и планов, которые составляются на основании и во исполнение:

– федеральных законов в области обеспечения информационной безопасности и защиты информации;

– постановлений Правительства Российской Федерации;

– руководящих, организационно-распорядительных и методических документов ФСТЭК России, ФСБ РФ, Роскомнадзора;

– руководящих и организационно - распорядительных документов КФУ;

– потребностей ИАС в средствах обеспечения безопасности информации.

15. Ожидаемый эффект от реализации Концепции

15.1. Реализация Концепции безопасности защищаемой информации в ИАС позволит:

– оценить состояние безопасности информации ИАС КФУ, выявить источники внутренних и внешних угроз информационной безопасности, определить приоритетные направления предотвращения, отражения и нейтрализации этих угроз;

– разработать распорядительные и нормативно-методические документы применительно к защищаемой информации, в том числе и к персональным данным;

– провести классификацию и сертификацию ИАС КФУ;

– провести организационно-режимные и технические мероприятия по обеспечению безопасности защищаемой информации;

– обеспечить необходимый уровень безопасности объектов защиты.

15.2. Осуществление этих мероприятий обеспечит создание единой, целостной, скоординированной, интегрированной системы информационной безопасности ИАС КФУ и создаст условия для ее дальнейшего совершенствования.

Начальник управления кадров  Д.Ш. Исрафилова

СОГЛАСОВАНО
Начальник Юридического управления


_____ Г. М. Сибгатуллина
(подпись)

СОГЛАСОВАНО
Проректор по административной работе - руководитель аппарата

_____ А. Н. Хашов
(подпись)