СОДЕРЖАНИЕ

1. ИНФОРМАЦИЯ О ДОКУМЕНТЕ	3
2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ.....	3
3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И НОРМАТИВНЫЕ ССЫЛКИ.....	3
4. ОБЛАСТЬ ПРИМЕНЕНИЯ	3
5. ОБЩИЕ ПОЛОЖЕНИЯ.....	4
6. ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	5
7. ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ.....	6
8. РЕАЛИЗАЦИЯ.....	7
9. КОНТРОЛЬ	8
10. СОВЕРШЕНСТВОВАНИЕ	8
Приложение № 1 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.....	10
Приложение № 2 НОРМАТИВНЫЕ ССЫЛКИ	16
Приложение № 3 ПОЛОЖЕНИЕ О ДОСТУПЕ К ИНФОРМАЦИОННЫМ РЕСУРСАМ ..	17
Приложение № 4 ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ.....	19
Приложение № 5 ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	21
Приложение № 6 ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ	23
Приложение № 7 ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТЫ.....	25
Приложение № 8 ПОЛОЖЕНИЕ О ЗАЩИТЕ ОТ ВРЕДНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ	27
Приложение № 9 ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ СРЕДСТВ БЕСПРОВОДНОГО ДОСТУПА.....	29
Приложение № 10 ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ УСТРОЙСТВ	31
Приложение № 11 ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ РАБОЧИХ МЕСТ	33
Приложение № 12 ПОЛОЖЕНИЕ О ТЕХНИЧЕСКОМ ОБСЛУЖИВАНИИ.....	35
Приложение № 13 ПОЛОЖЕНИЕ О КЛАСИФИКАЦИИ ИНФОРМАЦИИ	37
Приложение № 14 ПОЛОЖЕНИЕ ОБ ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ И СИСТЕМ.....	39
Приложение № 15 ПОЛОЖЕНИЕ ОБ УПРАВЛЕНИИ РОЛЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	41
Приложение № 16 ПОЛОЖЕНИЕ О МОНИТОРИНГЕ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	43
Приложение № 17 ПОЛОЖЕНИЕ О РЕАГИРОВАНИИ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.....	45
Приложение № 18 ПОЛОЖЕНИЕ О ФИЗИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ.....	47

1. ИНФОРМАЦИЯ О ДОКУМЕНТЕ

1.1. Назначение и правовая основа документа

Политика информационной безопасности ПФИЦ УрО РАН (далее – Политика) определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей, задач и способов защиты Информации в ПФИЦ УрО РАН.

Правила, процедуры, практические приемы и руководящие принципы в области информационной безопасности, которыми необходимо руководствоваться приведены в приложениях к Политике.

Основанием для дополнений и изменений в приложениях к Политике являются изменения целей, задач и правовых основ функционирования информационных систем ПФИЦ УрО РАН и эволюция угроз безопасности для объектов и субъектов информационных отношений ПФИЦ УрО РАН.

Законодательной основой настоящей Политики являются Конституция Российской Федерации, Гражданский и Уголовный кодексы, законы, указы, постановления, другие нормативные документы действующего законодательства Российской Федерации, документы Федеральной службы по техническому и экспортному контролю (ФСТЭК), Федеральной службы безопасности (ФСБ).

1.2. Доступ и периодичность пересмотра

Доступ: для внутреннего использования. Периодичность пересмотра - 3 года.

2. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие сокращения:

ИБ	– Информационная безопасность
ИС	– Информационная система
СУИБ	– Система управления информационной безопасностью
ОУС	– Объединенный ученый совет ПФИЦ УрО РАН

3. ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ И НОРМАТИВНЫЕ ССЫЛКИ

Термины и определения, используемые в настоящей Политике и рекомендуемые к использованию в нормативных и организационно-распределительных документах, созданных на её основе, приведены в Приложении №1 «Термины и определения».

При разработке настоящей Политики учтены требования и рекомендации, приведенные в приложении №2 «Нормативные ссылки».

4. ОБЛАСТЬ ПРИМЕНЕНИЯ

4.1. Настоящая Политика предназначена для установления единых норм, правил и требований к системе управления информационной безопасностью ПФИЦ УрО РАН.

4.2. Система управления ИБ является основной частью общей системы управления ПФИЦ УрО РАН, обеспечивает поддержку и управление процессами обеспечения ИБ на всех этапах деятельности корпоративной информационной системы.

4.3. Система обеспечения ИБ представляет собой совокупность нормативно-правовых, организационных и технических мер по обеспечению защищенности интересов ПФИЦ УрО РАН в информационной сфере, а также субъектов информационных отношений.

4.4. Основные цели системы управления ИБ ПФИЦ УрО РАН:

4.4.1. Разработка и поддержка административных, технических и физических мер безопасности для защиты конфиденциальности, целостности и доступности активов информационных систем, регулируемой и конфиденциальной информации.

4.4.2. Установление четкой ответственности за управление и использование информационных ресурсов.

4.4.3. Введение обоснованной и согласованной системы контроля и процедур по защите информации в структурных подразделениях, в информационно-технологических системах и сетях.

4.4.4. Обеспечение обучения и осведомленности сотрудников о своих обязанностях и понимание рисков в области информационной безопасности.

4.5. Положения настоящей Политики распространяются на все виды информации в ПФИЦ УрО РАН, хранящейся либо передающейся любыми способами, в том числе информацию, зафиксированную на материальных носителях.

4.6. Положение настоящей Политики также распространяются на средства приема, обработки, передачи, хранения и защиты информации ПФИЦ УрО РАН.

4.7. Политика применяется ко всем работникам ПФИЦ УрО РАН, а также к любой третьей стороне, включая лиц, работающих по договорам гражданско-правового характера и прикомандированных работников, имеющих доступ к информационным ресурсам ПФИЦ УрО РАН. Агенты и представители, осуществляющие деятельность от имени ПФИЦ УрО РАН, а также партнеры и клиенты ПФИЦ УрО РАН, консультанты и советники, подрядчики и поставщики – все обязаны соблюдать требования настоящей Политики.

4.8. Область применения настоящей Политики распространяется на все подразделения ПФИЦ УрО РАН, в которых обрабатывается информация, не составляющая государственную тайну.

5. ОБЩИЕ ПОЛОЖЕНИЯ

5.1. Информация – важный и жизненно необходимый ресурс ПФИЦ УрО РАН. Поэтому ПФИЦ УрО РАН защищает информацию так же надежно, как и любой другой ценный ресурс ПФИЦ УрО РАН. ПФИЦ УрО РАН не может достичь своих основополагающих целей, если работники не будут своевременно и в полном объеме получать информацию, необходимую для выполнения работы. Помимо этого, крайне важно минимизировать риски и ущерб, связанные с возможным раскрытием информации, её искажением и компрометацией.

5.2. Вся существенная информация в любой форме, приобретенная или полученная ПФИЦ УрО РАН и используемая для поддержки его законной деятельности, либо разработанная (созданная) работниками при выполнении служебных обязанностей, принадлежит ПФИЦ УрО РАН. Это право распространяется на информацию, передаваемую посредством голосовой, факсимильной и электронной связи с использованием аппаратуры ПФИЦ УрО РАН, на приобретённое и разработанное

программное обеспечение, на электронные почтовые ящики, а также на бумажные и электронные файлы (данные) работников, структурных подразделений, дочерних и контролируемых организацией.

5.3. Для защиты ресурсов своей корпоративной информационной системы и связанных с нею существенных данных от случайного или несанкционированного изменения, раскрытия или уничтожения, а также для обеспечения конфиденциальности, целостности и доступности информации и средств ее обработки ПФИЦ УрО РАН применяет меры по организованной безопасности и физической защите, технические меры безопасности, а том числе контроль доступа, криптографические технологии и другие технологии защиты информации. При этом мероприятия по охране и защите являются достаточными, законными и отвечают требованиям ПФИЦ УрО РАН в части законности деловых операций и соблюдения деловой этики. Настоящая Политика соответствует законодательству Российской Федерации, руководящим документам ФСБ и ФСТЭК России, внутренним документам в области безопасности.

5.4. Любое лицо, работающее на ПФИЦ УрО РАН, обязано поддерживать конфиденциальность и целостность деловой информации ПФИЦ УрО РАН и защищать эту информацию от несанкционированного, незаконного или случайного раскрытия, искажения или уничтожения.

5.5. Защита информационных ресурсов ПФИЦ УрО РАН является обязанностью всех работников ПФИЦ УрО РАН, а также лиц, работающих по договору гражданско-правового характера, и (или) любой третьей стороны, имеющей доступ к этим ресурсам. Лица, работающее на ПФИЦ УрО РАН, несут персональную ответственность за выполнение внутренних требований и правил информационной безопасности.

5.6. Знание и соблюдение требований настоящей Политики обязательно для всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы центра.

6. ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

6.1. Положения по информационной безопасности ПФИЦ УрО РАН (далее – «Положения») разрабатываются на основании Политики информационной безопасности ПФИЦ УрО РАН в целях создания, развития и совершенствования общей системы защиты информации ПФИЦ УрО РАН.

6.2. Положения по ИБ являются положениями к настоящей Политике.

6.3. Правила доступа к информационным ресурсам ПФИЦ УрО РАН определены в «Положении о доступе к информационным ресурсам» (Приложение № 3).

6.4. Правила использования паролей определены в «Положении об использовании паролей» (Приложение № 4).

6.5. Программное обеспечение в ПФИЦ УрО РАН используется в соответствии с «Положением об использовании программного обеспечения» (Приложение № 5).

6.6. Правила пользования ресурсами сети Интернет в ПФИЦ УрО РАН указаны в «Положении об использовании сети Интернет» (Приложение № 6).

6.7. Правила пользования электронной почтой ПФИЦ УрО РАН указаны в «Положении об использовании электронной почты» (Приложение № 7).

6.8. Правила защиты от вредоносных программ определены в «Положении о защите от вредоносного программного обеспечения» (Приложение № 8).

6.9. Правила использования средств беспроводного доступа приведены в «Положении об использовании средств беспроводного доступа» (Приложение № 9).

6.10. Правила пользования мобильными устройствами в ПФИЦ УрО РАН приведены в «Положении об использовании мобильных устройств» (Приложение № 10).

6.11. Правила и порядок организации рабочих мест определены в «Положении об организации рабочих мест» (Приложение № 11).

6.12. Общие правила технического обслуживания элементов информационных систем указаны в «Положении о техническом обслуживании» (Приложение № 12).

6.13. Правила классификации информационных ресурсов ПФИЦ УрО РАН в целях обеспечения соответствующего уровня их защиты определены в «Положении о классификации информации» (Приложение № 13).

6.14. Инвентаризация информационных систем ПФИЦ УрО РАН проводится в соответствии с «Положением об инвентаризации информационных ресурсов и систем» (Приложение № 14).

6.15. Перечень ролей информационной безопасности и правила управления ролями ИБ приведены в «Положении об управлении ролями информационной безопасности» (Приложение № 15).

6.16. Мониторинг информационной безопасности в ПФИЦ УрО РАН выполняется в соответствии с «Положением о мониторинге событий информации безопасности» (Приложение № 16).

6.17. Реагирование на инциденты ИБ в ПФИЦ УрО РАН осуществляется в соответствии с «Положением о реагировании на инциденты информационной безопасности» (Приложение № 17).

6.18. Меры по физической защите оборудования и данных предприятия в соответствии с «Положением о физической защите информационных ресурсов» (Приложение № 18).

6.19. Принятие новых Положений, а также пересмотр или отмена действующих Положений оформляется документально и утверждается приказом директора ПФИЦ УрО РАН.

6.20. Актуализация Положений осуществляется при изменении законодательной или нормативной базы в области ИБ, а также при изменении внутренней ситуации в ПФИЦ УрО РАН.

7. ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

7.1. Основной целью управления ИБ является защита интересов ПФИЦ УрО РАН и его работников в области информационной безопасности.

7.2. Основными задачами управления ИБ являются:

7.2.1. Анализ состояния ИБ ПФИЦ УрО РАН;

7.2.2. Выбор и внедрение мер обеспечения ИБ, адекватных целям и задачам деятельности ПФИЦ УрО РАН;

7.2.3. Контроль выполнения правил ИБ;

7.2.4. Документальное подтверждение предупреждающих и корректирующих мер обеспечения ИБ.

7.3. В основе управления ИБ ПФИЦ УрО РАН лежит подход, отраженный в модели деятельности в виде циклического процесса «планирование – реализация – контроль – совершенствование» (по ГОСТ Р ИСО/МЭК 27001:2006).

7.4. ПФИЦ УрО РАН осуществляет деятельность по управлению рисками, повышению осведомленности сотрудников и реагированию на инциденты в области ИБ. Регулярно, не реже одного раза в два года, производится анализ состояния рисков, связанных с ИБ. Защитные меры должны основываться на всесторонней оценке этих рисков и должны быть им соразмерны.

7.5. Всю ответственность за защиту своей информации и информационных ресурсов ПФИЦ УрО РАН возлагает на руководителей структурных подразделений. Руководители структурных подразделений ПФИЦ УрО РАН должны осуществлять эффективную реализацию правил информационной безопасности, распределять ресурсы и ответственность и обеспечивать выполнение установленных требований безопасности работниками подчиненного подразделения.

7.6. ОУС ПФИЦ УрО РАН предоставляет руководству ПФИЦ УрО РАН экспертные оценки и рекомендации по вопросам обеспечения информационной безопасности.

8. РЕАЛИЗАЦИЯ

Реализация системы управления ИБ осуществляется на основе четкого распределения ролей и ответственности в области информационной безопасности.

8.1. Структура и ответственность

8.1.1. Ответственное лицо, назначенное приказом директора ПФИЦ УрО РАН, руководит работами по внедрению и совершенствованию СУИБ, в том числе организует выполнение Положений по ИБ.

8.1.2. Руководство всеми видами деятельности по управлению ИБ в структурных подразделениях ПФИЦ УрО РАН осуществляют руководители этих подразделений. Они же несут ответственность за выполнение обязательств Положений по ИБ.

8.1.3. Функции администратора по ИБ возлагаются на штатных работников подразделений ПФИЦ УрО РАН, которые осуществляют свою деятельность во взаимодействии с другими подразделениями ПФИЦ УрО РАН. Координацию их деятельности по защите информации осуществляет ответственное лицо, назначенное приказом директора ПФИЦ УрО РАН.

8.1.4. Ответственность работников ПФИЦ УрО РАН за надлежащее выполнение требований и правил ИБ определена в положениях, правилах, регламентах и другие внутренних нормативных и организационно-распределительных документах ПФИЦ УрО РАН, а также указана в инструкциях пользователей.

8.1.5. Все работники ПФИЦ УрО РАН несут персональную (должностную, материальную, административную, уголовную) ответственность за свои действия или бездействие, которые повлекут за собой разглашение или утрату конфиденциальных (служебных, коммерческих, персональных) данных, а также нарушение нормального функционирования информационных систем, информационно-телекоммуникационной

сети ПФИЦ УрО РАН или ее отдельных компонентов, несанкционированный доступ к сети ПФИЦ УрО РАН или ее отдельным компонентам, несанкционированный доступ к информации либо нарушение авторских и смежных прав в соответствии с нормативными актами ПФИЦ УрО РАН и законодательством Российской Федерации.

8.2. Осведомленность и информирование

8.2.1. Для обеспечения эффективного функционирования СУИБ первостепенное значение имеет осведомленность работников ПФИЦ УрО РАН по вопросам информационной безопасности.

8.2.2. Перед началом работы в информационных системах ПФИЦ УрО РАН работники знакомятся с «Инструкцией пользователя информационных систем ПФИЦ УрО РАН».

8.2.3. Доведение правил ИБ до персонала всех уровней проводится: при приеме на работу; в ходе производственных совещаний, собраний, профессиональной подготовки персонала, тренингов по информационной безопасности; с помощью радио, прессы, внутреннего сайта, электронной почты и других технических средств; посредством размещения информации на информационных стендах в помещениях ПФИЦ УрО РАН.

8.3. Реагирование на инциденты безопасности

8.3.1. Реагирование на инциденты ИБ осуществляется в соответствии с «Положением о реагировании на инциденты информационной безопасности» (Приложение № 16).

9. КОНТРОЛЬ

9.1. Контроль соблюдения требований настоящей Политики возлагается на ответственное лицо, назначенное приказом директора ПФИЦ УрО РАН. При необходимости контролирующие функции выполняют также третьи лица и организации, действующие на законных основаниях.

9.2. Контроль за активностью Политики осуществляет ответственное лицо, назначенное приказом директора ПФИЦ УрО РАН.

9.3. Контроль в области информационной безопасности является частью работ по обеспечению ИБ ПФИЦ УрО РАН. Целью контроля ИБ является выявление угроз, предотвращение их реализации, минимизация возможного ущерба.

9.4. Объектами контроля ИБ являются информационные ресурсы ПФИЦ УрО РАН (информация, работники и другие субъекты доступа, системы и средства информационных технологий, а также средства защиты информации).

9.5. Контроль ИБ проводится в форме мониторинга ИБ, который выполняется в соответствии с «Положением о мониторинге событий информационной безопасности» (Приложение № 15).

10. СОВЕРШЕНСТВОВАНИЕ

10.1. Для совершенствования системы управления ИБ в ПФИЦ УрО РАН выполняется систематический анализ и оценивание действующих ситуаций в области информационной безопасности.

10.2. Анализ ИБ осуществляется на основе данных мониторинга в соответствии с «Положением о мониторинге событий ИБ».

10.3. В ситуациях, требующих оперативного реагирования, работа ведется согласно «Положению о реагировании на инциденты ИБ».

10.4. Обобщенные результаты анализа ИБ представляются на заседании ОУС ПФИЦ УрО РАН с целью их оценки и выработки согласованных рекомендаций, направленных на формирование и реализацию корректирующих и превентивных действий по совершенствованию системы управления ИБ ПФИЦ УрО РАН.

10.5. Рекомендации, принятые на заседании ОУС ПФИЦ УрО РАН, заносятся в протокол, который утверждается председателем ОУС ПФИЦ УрО РАН..

10.6. На основании утвержденного протокола ОУС ПФИЦ УрО РАН ответственные за ИБ работники ПФИЦ УрО РАН организуют подготовку проектов нормативных и организационно-распорядительных документов (положений, инструкций, регламентов и других), направленных на совершенствование СУИБ.

10.7. Нормативные и организационно-распорядительные документы по информационной безопасности разрабатываются в строгом соответствии с Политикой информационной безопасности ПФИЦ УрО РАН.

10.8. Нормативные и организационно-распределительные документы по информационной безопасности утверждаются приказами по ПФИЦ УрО РАН и рассылаются руководством ПФИЦ УрО РАН и руководителями подразделений.

10.9. ПФИЦ УрО РАН применяет следующий системный подход к обеспечению исполнения требований и правил по информационной безопасности:

10.9.1. Настоящая Политика информационной безопасности ПФИЦ УрО РАН считается официально принятым документом после его утверждения приказом директора ПФИЦ УрО РАН.

10.9.2. Разработка и внедрение нормативных и организационно-распорядительных документов по информационной безопасности проводится поэтапно.

10.9.3. Все нормативные и организационно-распорядительные документы по информационной безопасности могут быть приняты, отменены и пересмотрены отдельными приказами по ПФИЦ УрО РАН, а также уточнены и дополнены распоряжениями по отдельному структурному подразделению.

10.9.4. Внутренние документы подразделений ПФИЦ УрО РАН не должны противоречить Политике ИБ и иным документам по информационной безопасности, утвержденным приказом по ПФИЦ УрО РАН. При наличии расхождений и противоречий между документами по информационной безопасности, утвержденными приказами по ПФИЦ УрО РАН, и внутренними документами подразделений ПФИЦ УрО РАН – все документы, утвержденные приказами по ПФИЦ УрО РАН, имеют преимущественную силу.

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

Аудит информационной безопасности – систематический, независимый и документируемый процесс получения свидетельств деятельности по обеспечению информационной безопасности и установлению степени выполнения критериев информационной безопасности, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии информационной безопасности организации (ГОСТ Р 53114-2008).

Аутентификация пользователя – подтверждение того, что пользователь соответствует заявленному.

Безопасность информации (данных) – состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность (ГОСТ Р 53114-2008).

Безопасность информационной технологии – состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность информационной системы, в которой она реализована (ГОСТ Р 53114-2008).

Блокирование информации (данных) – временное прекращение сбора, систематизации, накопления, использования, распространения информации, в том числе ее передачи.

Владелец информационного ресурса – работник или структурное подразделение ПФИЦ УрО РАН, распоряжающееся информационным ресурсом, в том числе определяющий порядок доступа и его использования.

Вредоносная программа – программа, предназначенная для осуществления несанкционированного доступа и (или) воздействия на информацию или ресурсы информационных систем.

Доступ к информации (данным) – возможность получения и использования информации (данных).

Защищаемая информация (защищаемые данные) – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, установленными собственником информации.

Идентификация – присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов (ГОСТ Р 53114-2008).

Идентификация риска – процесс обнаружения, распознавания и описания рисков (ГОСТ Р 53114-2008).

Информационная безопасность – защищенность информационных систем (информации и обрабатывающей ее инфраструктуры) от любых случайных или

злонамеренных воздействий, результатом которых может являться нанесение ущерба самой информации, ее владельцам или инфраструктуре (согласно Политике ИБ ПФИЦ УрО РАН).

Примечания:

- 1) По ГОСТ Р ИСО/МЭК 27002-2012: **Информационная безопасность** – защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например, аутентичность, подотчетность, неотказуемость и надежность.
- 2) По ГОСТ Р 53114-2008: **Информационная безопасность организации** – состояние защищенности интересов организации в условиях угроз в информационной сфере.

Таким образом, понятие **информационная безопасность ПФИЦ УрО РАН** охватывает как процессы защиты, так и состояние защищенности информации, информационной инфраструктуры и интересов ПФИЦ УрО РАН в информационной сфере.

Интересы ПФИЦ УрО РАН в информационной сфере – обеспечение условий деятельности ПФИЦ УрО РАН, препятствующих проявлению недопустимых для деятельности рисков, связанных с информационной сферой ПФИЦ УрО РАН.

Информационная сфера ПФИЦ УрО РАН - сфера деятельности ПФИЦ УрО РАН (в том числе затрагивающая внешних по отношению к ПФИЦ УрО РАН лиц), связанная с созданием, преобразованием и потреблением информации и охватывающая информацию, информационную инфраструктуру, субъектов, осуществляющих сбор, формирование, распространение и использование информации и существующие между нами отношения (по ГОСТ Р 53114-2008).

Информационная инфраструктура – совокупность объектов информатизации, обеспечивающая доступ потребителя к информационным ресурсам (по ГОСТ Р 53114-2008).

Информационные процессы – процессы создания, сбора, обработки, накопления, хранения, поиска, передачи и уничтожения информации.

Информационные ресурсы – документы и массивы документов, содержащиеся в информационных системах (библиотеках, архивах, фондах, банках данных, информационных системах других видов).

Информационная система – система, представляющая собой совокупность информации, а также информационных технологий и технических средств, позволяющих осуществлять обработку информации с использованием средств автоматизации или без использования таких средств.

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

Инцидент информационной безопасности – любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность (по ГОСТ Р 53114-2008).

Примечание: Инцидентами ИБ являются, в частности:

- утрата услуг, оборудования или устройств;
- системные сбои или перезагрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;

- нарушение физических мер защиты;
- неконтролируемые изменения системы;
- сбои программного обеспечения и отказы технических средств;
- нарушение правил доступа.

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

Конфиденциальность информации (данных) – обязательное для соблюдения требование не допускать распространения информации без согласия владельца информации или наличия иного законного основания.

Конфиденциальная информация (данные, сведения): документированная информация, доступ к которой ограничивается в соответствии с законодательством. К конфиденциальным относятся сведения:

- а) о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);
- б) составляющие тайну следствия и судопроизводства;
- в) служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с ГК РФ и федеральными законами (служебная тайна);
- г) связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и т.д.);
- д) связанные с коммерческой деятельностью, доступ к которым ограничен в соответствии с ГК РФ и федеральными законами (коммерческая тайна);
- е) о сущности изобретения, исследования, разработки, модели или промышленного образца до официальной публикации информации о них.

Корпоративная информационная система – общая распределенная информационная система ПФИЦ УрО РАН, используемая для автоматизации процессов обработки информации и управления, реализуемая средствами информационных технологий и организационными мерами.

Управление ИБ ПФИЦ УрО РАН – скоординированные действия по руководству и управлению ПФИЦ УрО РАН в части обеспечения его информационной безопасности в соответствии с имеющимися условиями внутренней и внешней среды ПФИЦ УрО РАН (по ГОСТ Р 53114-2008).

Управление рисками ИБ ПФИЦ УрО РАН – скоординированные действия по руководству и управлению ПФИЦ УрО РАН в отношении рисков ИБ с целью их минимизации (по ГОСТ Р 53114-2008).

Меры обеспечения ИБ – совокупность действий, направленных на разработку и/или практическое применение способов и средств обеспечения информационной безопасности.

Мониторинг ИБ – непрерывное наблюдение за состоянием и поведением объектов ИБ с целью их контроля, оценки и прогноза в рамках управления ИБ.

Нарушители ИБ – физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при её обработке техническими средствами в информационных системах.

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

Носитель информации (данных) – физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, сигналов, технических решений и процессов, количественных характеристик физической величины.

Обеспечение ИБ ПФИЦ УрО РАН – деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности ПФИЦ УрО РАН или на минимизацию ущерба от возможной реализации таких угроз (ГОСТ Р 53114-2008).

Обработка информации (данных) – действия (операции) с информацией, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), блокирование, уничтожение информации.

Объект доверия: Объект, в отношении которого необходима уверенность в его безопасности.

Примечание: Примерами объектов доверия в области ИБ является: система, сервис (услуга) безопасности, процесс, используемые для обеспечения ИБ.

Объект доступа – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Объект защиты информации – информация либо носитель информации, или информационный процесс, которую (который) необходимо защищать в соответствии с целью защиты информации (ГОСТ Р 53114-2008).

Объект ИБ – компонент информационной сферы ПФИЦ УрО РАН, на который направлена деятельность по обеспечению ИБ.

Объект информатизации – 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 (ГОСТ Р 53114-2008).

Оценка риска – процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку (ГОСТ Р 53114-2008).

Политика – общее намерение и направление, официально выраженное руководством ((ГОСТ Р ИСО/МЭК 27002-2012).

Система управления информационной безопасностью (СУИБ) – часть общей системы управления ПФИЦ УрО РАН, основанная на использовании методов оценки рисков для разработки, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения информационной безопасности (по ГОСТ Р 53114-2008).

Примечание. Система управления включает в себя организационную структуру, политики, деятельность по планированию, распределение ответственности, практическую деятельность, процедуры, процессы и ресурсы (по ГОСТ Р 53114-2008).

Система обеспечения информационной безопасности – совокупность нормативно-правовых, организационных и технических мер по обеспечению

защищенности интересов в информационной сфере, а также субъектов информационных отношений.

Технические средства информационных систем – 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.

Пользователь информационной системы – лицо, участвующее в функционировании информационной системы либо использующее результаты её функционирования.

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

Программное воздействие – несанкционированное воздействие на ресурсы автоматизированной информационной системы, осуществляемое с использованием вредоносных программ.

Распространение информации (данных) – действия, направленные на передачу информации определенному кругу лиц или на ознакомление с информацией неограниченного круга лиц, в том числе обнародование в средствах массовой информации, размещение в информационно-телекоммуникационных сетях или предоставление доступа к информации каким-либо иным способом.

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

Риск – сочетание вероятности события и его последствий (ГОСТ Р ИСО/МЭК 27002-2012). Применительно к ИБ, риск – сочетание вероятности нанесения ущерба и тяжести этого ущерба.

Роль ИБ – совокупность прав, привилегий и ограничений на использование ресурсов корпоративной информационной системы, предоставляемая работникам ПФИЦ УРО РАН и третьим лицам на выполнения ими функциональных обязанностей.

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

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

Система защиты информации (данных) – совокупность организационных и технических мероприятий для защиты информации от неправомерного или случайного доступа, уничтожения, изменения, блокирования, копирования, распространения, а также иных неправомерных действий с ней.

Третья сторона – лица или организация, которые признаны независимыми от участвующих сторон, по отношению к рассматриваемой проблеме (ГОСТ Р ИСО/МЭК 27002-2012).

Угрозы безопасности информации (данных) – совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к

информации, результатом которого может стать её уничтожение, изменение, блокирование, копирование, распространение, а также иных несанкционированных действий при её обработке в информационных системах.

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

Целостность информации (данных) – способность средства вычислительной техники или информационной системы обеспечить неизменность информации в условиях её случайного и (или) преднамеренного искажения (разрушения).

НОРМАТИВНЫЕ ССЫЛКИ

При разработке настоящей Политики учтены требования и рекомендации следующих документов:

Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

Перечень сведений конфиденциального характера «Указ Президента РФ от 06.03.1997 г. N 188 с изменениями и дополнениями от 23.09.2005 г.».

Методический документ ФСТЭК России от 11.02.2014 г. «Меры защиты информации в государственных информационных системах».

Требования государственного регулятора в области информационной безопасности, указанные в письме в адрес ПФИЦ УрО РАН.

ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

ГОСТ Р 53114-2008. Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.

ГОСТ Р ИСО/МЭК 27002-2012. Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

ПОЛОЖЕНИЕ О ДОСТУПЕ К ИНФОРМАЦИОННЫМ РЕСУРСАМ

1. Назначение и область действия

1.1. Настоящее Положение о доступе к информационным ресурсам (далее «Положение») определяет основные правила и требования по обеспечению информационной безопасности информационных ресурсов ПФИЦ УрО РАН от любых форм неавторизованного доступа, использования и раскрытия информации.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Получение пользователями доступа к информационным ресурсам основывается на аутентификации этих пользователей и разграничении доступа.

2.2. В качестве объектов доступа рассматриваются информационные ресурсы ПФИЦ УрО РАН, в отношении которых ПФИЦ УрО РАН имеет право владения, распоряжения, пользования: данные (информация), технические средства, программные средства, услуги (сервисы) информационных систем.

2.3. Каждому пользователю сопоставляется учетная запись пользователя, присваиваются, по возможности, единые для различных объектов доступа ПФИЦ УрО РАН атрибуты информационной безопасности: уникальный идентификатор, «секрет» аутентификации, права доступа – с учетом их возможности и ценности для деятельности ПФИЦ УрО РАН.

2.4. В ПФИЦ УрО РАН могут применяться виды аутентификации, основанные на знании пользователем пароля (базовый вид аутентификации), на владении физическим носителем «секрета» (смарт-карты, устройства контактной памяти, USB-ключи, криптографические токены), на уникальных данных пользователя (биометрические параметры). При необходимости может использоваться комбинация двух и более видов.

2.5. Пользователи уведомляются об обязанностях по обращению с «секретами» аутентификации и сроках истечения их действия. «Секреты», в свою очередь передаются пользователям способом, исключающим несанкционированное ознакомление с ними. Передача пользователем личного «секрета» другому лицу запрещена.

2.6. Назначение прав доступа соответствует принципу «Запрещено все, что явно не разрешено» и определяется, исходя из служебных обязанностей пользователя.

2.7. Категорически запрещен доступ к ресурсам по принципу «Всем – Полный доступ». Запрещен также неавторизованный (анонимный, гостевой) доступ к любым ресурсам, кроме общедоступных страниц веб-сайтов ПФИЦ УрО РАН.

2.8. Пересмотр прав доступа осуществляется при возникновении производственной необходимости и документируется.

2.9. Управление доступом к сетевым информационным ресурсам и услугам производится, в том числе, путем разделения информационной телекоммуникационной системы ПФИЦ УрО РАН на отдельные логические и физические сетевые сегменты.

2.10. В ПФИЦ УрО РАН должны использоваться средства контроля над соблюдением правил доступа к объектам доступа.

2.11. Служебный доступ к объектам доступа ПФИЦ УрО РАН, осуществляемый по внешним каналам связи, должен защищать с применением механизмов аутентификации и криптографической защиты информации.

2.12. Доступ к общедоступным страницам веб-сайтов ПФИЦ УрО РАН не требует соблюдения требований раздела 2.11, достаточно обеспечить шифрование трафика.

2.13. Для снижения вероятности угроз несанкционированного доступа, необходимо минимизировать число устройств, имеющих легальные внешние IP-адреса сети Интернет. Оборудование, имеющее легальные внешние IP-адреса сети Интернет, должно проверять на наличие уязвимостей и автоматически получать обновления безопасности.

2.14. Объекты доступа ПФИЦ УрО РАН должны быть защищены от внешних угроз из сети Интернет и из локальной сети сетевыми брандмауэрами и штатными средствами защиты, входящими в состав операционной системы и приложений. Число открытых для доступа сервисов и ресурсов на этих объектах должно быть минимально необходимым.

2.15. В договорах с поставщиками информационно-технических услуг определяют требования по управлению доступом к этим услугам.

2.16. При увольнении работника обеспечивается невозможность его доступа к объектам доступа ПФИЦ УрО РАН.

2.17. При нарушении требований данного Положения доступ пользователя к информационным ресурсам может быть временно заблокирован ответственными лицами (см. раздел 3.2) до устранения нарушения.

2.18. Порядок работы с информационными ресурсами, содержащими сведения, отнесенные к государственной тайне либо к персональным данным, защита которых организуется в соответствии с требованиями законодательства РФ, определяется соответствующими внутренними документами ПФИЦ УрО РАН. Разработка и утверждение этих документов производится вне настоящего Положения.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителя подразделения ПФИЦ УрО РАН; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ

1. Назначение и область действия

1.1. Настоящее Положение об использовании паролей (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности ПФИЦ УрО РАН от угроз, связанных с некорректным использованием средств аутентификации (паролей).

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, имеющих доступ или ответственных за предоставление доступа к любой информационной системе ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Пользовательские пароли (для доступа к электронной почте, сети, компьютеру и т.д.) должны содержать не менее шести буквенно-цифровых символов (буквы латинского алфавита, цифры).

2.2. Административные пароли (административных учетных записей операционных систем, телекоммуникационного оборудования, баз данных, информационных систем и т.д. (должны содержать не менее восьми буквенно-цифровых символов и спецсимволов, если они поддерживаются программным обеспечением (буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы типа ! @ # \$ % ^ & * _ =).

2.3. Для простоты запоминания могут быть использованы парольные фразы, разделенные спецсимволами и цифрами.

2.4. Пароль не должен совпадать с логином пользователя (наименованием учетной записи) и содержать легко угадываемые слова и числа (имена, даты рождения, номера документов и т.п.).

2.5. Пользователи лично ответственны за выбор пароля, отвечающего заданным критериям сложности, и за его хранение, исключаящее ознакомление с ним третьих лиц.

2.6. Запрещается передача паролей третьим лицам.

2.7. Запрещается запись и хранение паролей в местах, где они могут быть легко доступны и прочитаны.

2.8. Все пользовательские пароли должны заменяться не реже одного раза в год. Рекомендованный интервал – шесть месяцев.

2.9. Все административные пароли должны заменяться не реже одного раза в полгода. Рекомендованный интервал – три месяца.

2.10. Запрещается отправлять пароли в сообщениях электронной почты, SMS или через другие формы электронного обмена информацией, кроме специально оговоренных случаев (одноразовые пароли с ограниченным сроком действия; пароли, создаваемые самим пользователем при помощи средств электронного обмена информацией и т.п.).

2.11. Доступ к общедоступным страницам веб-сайтов центра не требует паролей защиты.

2.12. В случае компрометации пароля (утраты, хищения и т.п.), пользователь должен немедленно сменить пароль. Если пользователь не имеет возможности самостоятельно сменить пароль, администратор заменяет его пароль новым паролем, который сообщает пользователю.

2.13. Учетные записи пользователей, чьи пароли не соответствуют требованиям настоящего Положения, могут быть заблокированы ответственными лицами (см. раздел 3.2).

3. Роли и ответственность

3.1. Ответственность за соблюдение требований разделов 2.1-2.12 данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений ПФИЦ УрО РАН. Ответственность за обеспечение технической возможности выполнения требований разделов 2.1-2.12 и за соблюдение требований разделов 2.1-2.13 возлагается на: работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Назначение и область действия

1.1. Настоящее Положение об использовании программного обеспечения (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности ПФИЦ УрО РАН от угроз, связанных с использованием программного обеспечения (далее – «ПО»).

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для использования.

2. Основные требования

2.1. В ПФИЦ УрО РАН разрешается использовать следующие виды ПО:

2.1.1. ПО, разработанные в ПФИЦ УрО РАН для обеспечения уставной деятельности ПФИЦ УрО РАН;

2.1.2. ПО, законно приобретенное или полученное ПФИЦ УрО РАН на основании договорных или лицензированных соглашений с разработчиком либо правообладателем;

2.1.3. «свободное» ПО, распространяемое с открытым исходным кодом (Open Source) либо под свободными лицензиями: GPL, LGPL, BSD, Apache и аналогичными;

2.1.4. «бесплатное» ПО, лицензия на которое явно допускает его безвозмездное использование в корпоративной среде (в коммерческих целях, на служебных компьютерах, для выполнения должностных обязанностей и т.р.). При этом обязательно наличие текста такой лицензии на русском языке.

2.2. Доступ пользователей к системному и прикладному ПО должен быть санкционирован и разрешен непосредственным руководителем только для выполнения служебных обязанностей.

2.3. Пользователям **ЗАПРЕЩЕНО**:

2.3.1. получать (приносить, скачивать), хранить, устанавливать и использовать нелегальное программное обеспечение;

2.3.2. использовать программное и аппаратное обеспечение ПФИЦ УрО РАН в неслужебных (личных) целях;

2.3.3. использовать административные учетные записи за исключением обстоятельств, когда без этого невозможно выполнение или должностных обязанностей;

2.3.4. использовать административные учетные записи без пароля;

2.3.5. устанавливать и использовать программное обеспечение, которое не требуется им для выполнения должностных обязанностей.

2.4. Пользователи могут самостоятельно устанавливать и обновлять необходимое для работы ПО на своих рабочих местах после согласования с руководством. При этом

каждый пользователь несет персональную ответственность за ПО, установленное на его рабочей станции.

2.5. Бездействующие сеансы работы должны автоматически блокироваться после определенного периода бездействия. Если автоматическое блокирование рабочего сеанса не настроено, пользователь должен самостоятельно блокировать свой сеанс, отходя от компьютера.

2.6. Для обеспечения корректной работы ПО рекомендуется применять системы автоматического обновления ПО. Критические обновления безопасности ПО подлежат обязательному распространению во всех информационных системах ПФИЦ УрО РАН.

2.7. Необходимо регулярно проверять установленное в центре ПО на предмет соблюдения авторских и смежных прав на интеллектуальную собственность.

2.8. Требования к представителям сторонних организаций, использующих в своей деятельности ПО ПФИЦ УрО РАН, должны включаться в соответствующие договора.

2.9. ПО, установленное или используемое в ПФИЦ УрО РАН в нарушение настоящего Положения, может быть заблокировано или удалено ответственными лицами (см. раздел 3.2).

3. Роли и ответственность

3.1. Ответственность за соблюдение требований разделов 2.1-2.5 данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих в своей деятельности в ПФИЦ УрО РАН программное обеспечение.

3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений ПФИЦ УрО РАН. Ответственность за обеспечение технической возможности выполнения требований разделов 2.1-2.5 и за соблюдение требований разделов 2.1-2.9 возлагается на: работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ

1. Назначение и область действия

1.1. Настоящее Положение об использовании сети Интернет (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности ПФИЦ УрО РАН от угроз, связанных с воздействием программ из сети Интернет, специально разработанных или модифицированных для несанкционированного уничтожения, блокирования, модификации либо копирования информации, а также нарушения нормального функционирования элементов ИС ПФИЦ УрО РАН.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН для доступа в сеть Интернет. Является обязательным для исполнения.

2. Основные требования

2.1. Доступ работника к сети Интернет должен быть санкционирован непосредственным руководителем.

2.2. Доступ в сеть Интернет для участников конференций, семинаров, иных мероприятий возможен при наличии заявки в адрес администратора сегмента сети от лица, ответственного за проведение мероприятия.

2.3. Доступ к сети Интернет должен быть разрешен только для выполнения служебных обязанностей и не может использоваться для ненадлежащей или незаконной деятельности.

2.4. При работе в сети Интернет запрещается передавать информацию ограниченного доступа (персональные данные, коммерческая и служебная информация) без соответствующего разрешения и надлежащей защиты (Шифрование, пароли, электронная подпись).

2.5. При использовании сети Интернет в ПФИЦ УрО РАН необходимо соблюдать законодательные, регулирующие и контрактные требования в отношении авторских и смежных прав на интеллектуальную собственность в области программного обеспечения, а также в отношении научных, литературных, музыкальных, кинематографических и иных произведений, работ, трудов и материалов.

2.6. Запрещается посещать ресурсы сети Интернет, противоречащие законодательству РФ, в том числе: пропагандирующие насилие или экстремизм; разжигающие расовую, национальную или религиозную вражду; разъясняющие порядок изготовления и (или) применения наркотиков, взрывчатых веществ, оружия и т.п.; содержащие материалы порнографического характера; предназначенные для распространения компьютерных вирусов и других вредоносных программ; нарушающие

авторские и смежные права; предназначенные для подбора паролей и серийных номеров, для взлома и иной модификации программного обеспечения.

2.7. В ПФИЦ УрО РАН должен проводиться мониторинг информации, применяемой и передаваемой посредством сети Интернет с использованием информационных систем ПФИЦ УрО РАН.

2.8. Требования к представителям сторонних организаций, использующих в своей деятельности системы ПФИЦ УрО РАН для доступа в сеть Интернет, должны включаться в соответствующие договора.

2.9. Лица, ответственные за обеспечение и контроль доступа в сеть Интернет (см. раздел 3.2), могут временно блокировать доступ в сеть Интернет для пользователей, допустивших нарушения данного Положения.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников центра и третьих лиц, использующих в своей деятельности информационные системы ПФИЦ УрО РАН для доступа в сеть Интернет.

3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений ПФИЦ УрО РАН. Ответственность за обеспечение и контроль доступа в сеть Интернет возлагается на: работников, выполняющих функции администраторов систем доступа в сеть Интернет; работников, ответственных за администрирование сегмента информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТЫ

1. Назначение и область действия

1.1. Настоящее Положение об использовании электронной почты (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности при использовании электронной почты путем защиты целостности, конфиденциальности, доступности и достоверности информации ПФИЦ УрО РАН, передаваемой и принимаемой средствами электронной почты.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, взаимодействующих с ПФИЦ УрО РАН посредством электронной почты либо использующих средства и системы электронной почты ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Доступ работника к электронной почте ПФИЦ УрО РАН должен быть санкционирован непосредственно руководителем.

2.2. Получение или смена адреса электронной почты для работника обеспечивается ответственным лицом после получения подписанной руководителем заявки на создание или изменение адреса электронной почты.

2.3. Все входящие и исходящие сообщения электронной почты должны проверяться на наличие вредоносных программ.

2.4. При использовании электронной почты в ПФИЦ УрО РАН запрещается передавать информацию ограниченного доступа (персональные данные, коммерческая и служебная информация) без соответствующего разрешения и надлежащей защиты (шифрование, пароли, электронная подпись).

2.5. Запрещается отправка пользователями и пересылка почтовыми серверами ПФИЦ УрО РАН исполняемых, служебных и системных файлов, модулей и компонентов операционных систем и приложений.

2.6. Все факты отправки и приема электронных сообщений в ПФИЦ УрО РАН фиксируются.

2.7. При увольнении работника доступ к его электронной почте блокируется. Удаление адреса и содержимого электронной почты уволенного работника производится ответственным лицом по заявке руководителя работника.

2.8. При нарушении указанных в данном Положении правил работы с электронной почтой доступ работника к электронной почте может быть временно приостановлен ответственными лицами (см. раздел 3.2) до устранения нарушения.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные системы электронной почты ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; работников, выполняющих функции администраторов систем электронной почты; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН, работников, выполняющих функции администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ О ЗАЩИТЕ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

1. Назначение и область действия

1.1. Настоящее Положение о защите от вредоносного программного обеспечения (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности ПФИЦ УрО РАН от угроз, связанных с воздействием программ, разработанных или модифицированных для несанкционированного уничтожения, блокирования, модификации либо копирования информации, а также нарушения функционирования элементов информационных систем ПФИЦ УрО РАН.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Средства защиты от вредоносного программного обеспечения (далее – «ВПО») должны быть установлены, настроены и активизированы на всех допускающих такую установку программно-технических средствах до начала их работы с информационными системами ПФИЦ УрО РАН.

2.2. Средства защиты от ВПО должны иметь все последние обновления, полученные из доверенных источников.

2.3. Контролю на предмет обнаружения ВПО должна подвергаться вся информация, создаваемая и (или) обрабатываемая программно-техническими средствами, а также принимаемая и (или) передаваемая с помощью машинных носителей или средств телекоммуникаций.

2.4. В соответствии с «Положением об использовании программного обеспечения», в ПФИЦ УрО РАН разрешается использовать только лицензированные, свободные или бесплатные средства защиты от ВПО. Запрещено использовать средства защиты от ВПО, не имеющие требуемых лицензий либо модифицированные с целью снятия лицензионных ограничений.

2.5. Необходимо разработать перечень средств защиты от ВПО, чтобы их состав, архитектура и конфигурация могли быть рекомендованы в качестве общего решения для всех подразделений ПФИЦ УрО РАН.

2.6. Процессы установки, настройки, эксплуатации и обновления средств защиты от ВПО должны протоколироваться и контролироваться.

2.7. Программно-технические средства (компьютеры, серверы, коммуникационное оборудование и т.д.), допускающие установку средств защиты от ВПО, но не имеющие таковых, могут быть временно отключены от информационных систем и

сегментов локальных вычислительных сетей ПФИЦ УрО РАН ответственными лицами (см. раздел 3.2) при расследовании угроз безопасности, вирусных и иных атак.

3. Роли и ответственность

3.1. Ответственность за соблюдение требований разделов 2.1-2.4 данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений ПФИЦ УрО РАН. Ответственность за обеспечение технической возможности выполнения требований разделов 2.1-2.4 и за соблюдение требований разделов 2.1-2.7 возлагается на: работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ СРЕДСТВ БЕСПРОВОДНОГО ДОСТУПА

1. Назначение и область действия

1.1. Настоящее Положение об использовании средств беспроводного доступа (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности при эксплуатации беспроводных сетей ПФИЦ УрО РАН.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Приказом по ___ №__ утвержден «Регламент принятия решений на установку, ввод в эксплуатацию и вывод из эксплуатации технических средств беспроводной передачи данных и радиосвязи», которым необходимо руководствоваться при построении беспроводных сетей ___

2.2. Беспроводной доступ к информационным системам и ресурсам ПФИЦ УрО РАН для работников ПФИЦ УрО РАН и командированных разрешается при соблюдении требований безопасности.

2.3. Беспроводной доступ для участников конференций, семинаров, мероприятий разрешается исключительно для выхода в сеть Интернет.

2.4. Логин и пароль для беспроводного доступа выдается в соответствии с «Положением об использовании паролей»:

2.4.1. Для работников ПФИЦ УрО РАН – по заявке руководителя подразделения. Срок действия пароля – не более одного года (рекомендуется 6 месяцев);

2.4.2. Для участников конференций, семинаров, мероприятий – по заявке лица, ответственного за мероприятие. Срок действия пароля – до завершения мероприятия;

2.4.3. Для командированных и третьих лиц, выполняющих работы на территории ПФИЦ УрО РАН – по заявке руководителя соответствующего подразделения. Срок действия пароля – до завершения командировки либо работ.

2.5. Планируемая техническая реализация беспроводного доступа:

2.5.1. Унификация оборудования Wi-Fi для всех подразделений.

2.5.2. Использование двух частотных диапазонов: 2,4 и 5,0 ГГц.

2.5.3. Обслуживание точками доступа Wi-Fi трех VLAN (виртуальных подсетей): общедоступная, служебная (закрытая), управляющая.

2.5.4. Перепрограммирование роутеров Wi-Fi в режим коммутатора, для обеспечения в дальнейшем централизованной регистрации и блокировки подключенных устройств по MAC-адресу.

2.5.5.Регистрация MAC-адресов подключенных устройств с целью с целью предотвращения несанкционированного доступа.

2.5.6.Поддержка протокола шифрования WPA2, возможность авторизации устройств на сервере авторизации.

2.6. При работе в беспроводных сетях ПФИЦ УрО РАН необходимо также руководствоваться «Положением об использовании мобильных устройств».

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих беспроводные средства передачи данных ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; ответственных за исполнение «Регламента принятия решений на установку, ввод в эксплуатацию и вывод из эксплуатации технических средств беспроводной передачи данных и радиосвязи»; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ УСТРОЙСТВ

1. Назначение и область действия

1.1. Настоящее Положение об использовании мобильных устройств (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности при эксплуатации мобильных устройств обработки информации ПФИЦ УрО РАН. К мобильным устройствам обработки информации относятся: ноутбуки, карманные мини-компьютеры, электронные планшеты, смартфоны и иные носимые устройства, которые можно использовать для получения, записи, обработки, хранения и передачи информации.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, взаимодействующих с ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Порядок вноса в административные здания ПФИЦ УрО РАН и выноса из них мобильных устройств обработки информации регламентируется внутренними документами ПФИЦ УрО РАН в части требований к проходу с телевизионной, фото, видео, звукозаписывающей и радиоэлектронной аппаратуры, а также перемещению имущества и грузов через контрольно-пропускные пункты.

2.2. Не допускается использование мобильных устройств обработки информации для осуществления звуковой и видеозаписи или ретрансляции переговоров и совещаний по вопросам, затрагивающим конфиденциальную информацию ПФИЦ УрО РАН.

2.3. Работники, осуществляющие эксплуатацию мобильных устройств обработки информации для хранения и обработки конфиденциальной информации ПФИЦ УрО РАН, обязаны:

2.3.1. знать и соблюдать требования локальных нормативных актов ПФИЦ УрО РАН по обеспечению информационной безопасности и инструкций по эксплуатации средств защиты информации;

2.3.2. использовать все доступные защитные механизмы для предотвращения доступа к конфиденциальной информации ПФИЦ УрО РАН посторонних лиц;

2.3.3. не хранить конфиденциальную информацию ПФИЦ УрО РАН в открытом виде вне работы с ней, а также во время соединения с другими информационными системами;

2.3.4. не допускать передачу конфиденциальной информации ПФИЦ УрО РАН по открытым каналам связи без принятия мер по ее криптографической защите;

2.3.5. своевременно информировать руководство и ответственных лиц (см. раздел 3.2) о фактах утечки конфиденциальной информации ПФИЦ УрО РАН, утраты портативных средств защиты (доступ к ним посторонних лиц, а также подозрение на такой

доступ), разглашения идентификаторов доступа к информационным системам ПФИЦ УрО РАН и т.д.;

2.3.6. при прекращении использования мобильного средства обработки информации или при передаче его другому лицу – обеспечить уничтожение содержащейся в нем конфиденциально информации ПФИЦ УрО РАН.

3. Роль и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих мобильные устройства обработки информации для работы с информационными ресурсами и системами ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; работников, участвующих в реализации пропускного режима; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ РАБОЧИХ МЕСТ

1. Назначение и область действия

1.1. Настоящее Положение об организации Рабочих мест (далее – «Положение») определяющий процесс организации рабочих мест для безопасности работы работников ПФИЦ УрО РАН.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. При приеме на работу, при смене рабочего места, при изменении должностных обязанностей работника – руководитель подразделения (при необходимости) заранее оформляет заявку в произвольном виде на организацию рабочего места пользователя с указанием потребностей и направляет её ответственному лицу.

2.2. Выполнение заявки на обеспечение или изменение доступа пользователей включает в себя назначение прав доступа к сетевым ресурсам локальной сети, сети Интернет, электронной почте ПФИЦ УрО РАН, программному обеспечению, базам данных, телефонной связи.

2.3. Выполнение заявки при необходимости согласует руководитель структурного подразделения.

2.4. С целью снижения рисков сбоя вследствие возможной недостаточной компьютерной грамотности нового работника, первый рабочий сеанс нового работника может производиться под контролем руководителя или ответственного лица.

2.5. В случае необходимости закрытия доступа пользователя к информационным ресурсам, руководитель подразделения заранее направляет заявку в произвольном виде в адрес ответственного лица. На основании заявки в течение одного рабочего дня блокируется учетная запись пользователя, а также закрывается доступ к сетевым ресурсам, информационным системам, электронной почте, сети Интернет.

2.6. В случае возможности ознакомления неавторизованным лицом с конфиденциальной информацией, предоставленной на экране компьютера или бумажном носителе в присутствии авторизованного пользователя, последний должен предпринять необходимые меры по предотвращению такого ознакомления.

2.7. В случае отсутствия на непродолжительное время на своем рабочем месте, пользователь должен заблокировать доступ к своему компьютеру, обеспечить отсутствие информации на экране (или завершить сеанс работы), а также предпринять соответствующие меры по защите конфиденциальной информации на физических носителях.

2.8. Применяемые меры по обеспечению безопасности при хранении физических носителей информации должны соответствовать категории хранимо на них информации.

2.9. Конфиденциальная информация после печати должна незамедлительно изыматься из принтера для ее защиты от неавторизованного прочтения.

2.10. Плакаты, информационные стенды и документы, содержащие конфиденциальную информацию, по окончании их использования должны помещаться в специальное хранилище либо уничтожаться.

2.11. Надписи при проведении совещаний, оставленные на демонстрационных досках, должны удаляться после окончания совещания.

2.12. Пользователям запрещается без согласования с руководством использовать на рабочих местах оборудование и программное обеспечение, которые не принадлежат ПФИЦ УрО РАН на правах собственности, аренды, пользования, либо в отношении которых ПФИЦ УрО РАН не обладает иными (в том числе неисключительными) правами.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ О ТЕХНИЧЕСКОМ ОБСЛУЖИВАНИИ

1. Назначение и область действия

1.1. Настоящее Положение о техническом обслуживании (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности ПФИЦ УрО РАН от угроз, связанных с нарушением непрерывности деятельности ПФИЦ УрО РАН в целом, вызванных неисправностями оборудования и кабельных линий.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Техническое обслуживание и ремонт оборудования и кабельной линий (электропитания и телекоммуникации) производится только уполномоченными на это работниками (персоналом соответствующих подразделений и обслуживающим персоналом) и документируется.

2.2. Техническое обслуживание и ремонт оборудования и кабельных линий проводится регулярно в соответствии с регламентом технического обслуживания и с учетом требований страхования (при его наличии) и гарантийного обслуживания.

2.3. Техническое обслуживание и ремонт оборудования и кабельных линий проводится таким образом, чтобы исключить или минимизировать риски потери функциональности корпоративной информационной системы. На период технического обслуживания и ремонта оборудование, поддерживающие критические рабочие и вычислительные процессы, рекомендуется заменять резервным.

2.4. В программно-технических средствах, направленных для технического обслуживания и ремонта, вся конфиденциальная информация (данные и программы) после переноса на другие носители уничтожается способом, обеспечивающим невозможность ее восстановления.

2.5. Все устройства хранения информации перед утилизацией проверяется на наличие конфиденциальной информации. При наличии таковой, они уничтожаются по акту способом, гарантирующим невозможность восстановления ранее хранящейся информации.

2.6. выявленные в процессе технического обслуживания отклонения и неисправности регистрируются и устраняются немедленно либо (при необходимости) заносятся в план по ремонту.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений ПФИЦ УрО РАН; работников, отвечающих за техническое обслуживание и ремонт вычислительной техники и кабельных линий ПФИЦ УрО РАН.

ПОЛОЖЕНИЕ О КЛАССИФИКАЦИИ ИНФОРМАЦИИ

1. Назначение и область действия

1.1. Настоящее Положение о Классификации информации (далее – «Положение») определяет основные правила и требования по классификации информационных ресурсов ПФИЦ УрО РАН с точки зрения их ценности (важности) и критичности для деятельности ПФИЦ УрО РАН в целях обеспечения адекватного уровня их защиты.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения

2. Основные требования

2.1. Для обеспечения уровней защиты информационных ресурсов, адекватных потребностям деятельности ПФИЦ УрО РАН, они классифицируются в соответствии со степенью важности содержащейся в них информации.

2.2. Информационные ресурсы ПФИЦ УрО РАН классифицируются в соответствии со следующими тремя категориями:

I – содержит **конфиденциальные** сведения (основные требования к обеспечению конфиденциальности, целостности и доступности информационных ресурсов);

II – содержит сведения **для внутреннего пользования** (минимально достаточные требования: парольная защита, хранение носителей информации с ограничением доступа третьих лиц);

III – содержит **общедоступные** сведения (требования по защите не предъявляются).

2.3. Порядок работы с информационными ресурсами, содержащими сведения, отнесенные к государственной тайне, защита которых организуется в соответствии с требованиями законодательства РФ, определяется соответствующими внутренними документами ПФИЦ УрО РАН. Разработка и утверждение этих документов производится вне настоящего Положения.

2.4. Перечень конфиденциальных сведений утвержден приказом директора ПФИЦ УрО РАН «Об утверждении Перечня сведений, подлежащих отнесению к конфиденциальной информации ПФИЦ УрО РАН.

2.5. В ПФИЦ УрО РАН информация категории I (конфиденциальная) подразделяется на:

2.5.1. информацию, составляющую служебную и коммерческую тайну;

2.5.2. персональные данные, защита которых организуется в соответствии с требованиями законодательства РФ.

2.6. Конфиденциальная информация, составляющая служебную и коммерческую тайны:

2.6.1. не подлежит передаче по открытым каналам передачи данных и в открытой переписке без принятия мер защиты;

2.6.2. не сообщается в личных и деловых переговорах по открытым каналам связи;

2.6.3. не публикуется в средствах массовой информации до принятия решений об ее публикации.

2.7. Использование персональных данных в деятельности ПФИЦ УрО РАН производится только с согласия их владельца. Порядок использования персональных данных определяется соответствующими внутренними документами ПФИЦ УрО РАН, разработка и утверждение которых производится вне настоящего Положения.

2.8. Присвоение информационным ресурсам классификационные категории подвергаются периодическому пересмотру. Информационные ресурсы при необходимости снабжаются соответствующей маркировкой.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ ОБ ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ И СИСТЕМ

1. Назначение и область действия

1.1. Настоящее Положение об инвентаризации информационных ресурсов и систем (далее «Положение») определяет основные правила и требования по инвентаризации информационных ресурсов и систем ПФИЦ УрО РАН с точки зрения их ценности (важности) и критичности для деятельности ПФИЦ УрО РАН в целях обеспечения адекватного уровня их защиты.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Все информационные ресурсы и системы ПФИЦ УрО РАН подлежат инвентаризации с документирование ресурсов в соответствующем реестре.

2.2. Инвентаризации подлежат следующие типы информационных систем: групповые ИС (используемые коллективно членами группы или подразделения); ИС обработки данных; распределенные файл-серверные либо клиент-серверные ИС, корпоративная ИС и т.д.

2.3. Инвентаризации подлежат следующие типы информационных ресурсов, а также технических и программных средств: базы и файлы данных; компьютерное оборудование, аппаратура связи, технические средства обеспечения ИБ, копировальные и печатающие устройства, носители информации, установки электроснабжения, кондиционирования воздуха и т.д.; системное и прикладное программное обеспечение, средства разработки и технологические программы, программные средства обеспечения ИБ; услуги информационно-технологического обеспечения: доступ к данным, обработка и передача данных, телефонная, видео- и конференцсвязь.

2.4. В реестре информационных ресурсов и систем, технических и программных средств отражаются следующие атрибуты: наименование, владелец, либо лицо, которому делегировано право распоряжения, администратор, пользователи, местоположение, категория информационного ресурса, степень конфиденциальности.

2.5. Актуальность реестра обеспечивается на основе непрерывного официального процесса его поддержки.

2.6. Должны быть разработаны и внедрены планы поддержки или восстановления работы и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или отказа процессов, критичных для деятельности ПФИЦ УрО РАН.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы системы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ ОБ УПРАВЛЕНИИ РОЛЯМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Назначение и область действия

1.1. Настоящее Положение об управлении ролями информационной безопасности (далее «Положение») определяет основные роли, связанные с обеспечением информационной безопасности ПФИЦ УрО РАН.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Ролями информационной безопасности являются согласованные функциональные обязанности, права и ответственность.

2.2. Для обеспечения требуемой согласованности ролей необходимо исключить возможность существования процессов по обеспечению информационной безопасности, не поддерживаемых ни одной ролью ИБ, а также исключить возможность пересечения различных ролей ИБ.

2.3. Распределение ролей соответствует принятым в ПФИЦ УрО РАН правилам и требованиям информационной безопасности, а также учитывает сложившуюся практику ПФИЦ УрО РАН.

2.4. В ПФИЦ УрО РАН определяются и распределяются следующие основные роли информационной безопасности:

- 2.4.1. Владелец информационного ресурса;
- 2.4.2. Пользователь информационного ресурса;
- 2.4.3. Администратор информационного ресурса;
- 2.4.4. Администратор информационной безопасности;
- 2.4.5. Аудитор информационной безопасности;
- 2.4.6. Третьи лица.

2.5. Роли информационной безопасности обеспечиваются ресурсами, необходимыми и достаточными для выполнения их обязанностей.

2.6. Персональные обязанности, ответственность и права лиц, исполняющих роли информационной безопасности, определяются законодательством РФ, уставными документами центра, приказами, договорами, положениями, руководствами, инструкциями и доводятся до сведения исполнителя роли.

2.7. В зависимости от вида и тяжести нанесенного ущерба, исполнитель роли информационной безопасности может нести административную, материальную, дисциплинарную и уголовную ответственность.

3. Роль и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ О МОНИТОРИНГЕ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Назначение и область действия

1.1. Настоящее Положение о мониторинге событий информационной безопасности (далее – «Положение») определяет основные правила и требования по оперативному сбору, анализу, обобщению и сравнению текущих и эталонных параметров информационной безопасности ПФИЦ УрО РАН.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Мониторинг информационной безопасности проводится с целью выявления нецелевого использования средств обработки информации пользователями, несанкционированных действий работников и авторизованных третьих лиц в корпоративной информационной системе ПФИЦ УрО РАН, оперативного реагирования на инциденты информационной безопасности, сбора данных и проведения служебных расследований.

2.2. Для целей мониторинга информационной безопасности используются специализированные средства и штатные (входящие в состав информационных систем) средства контроля доступа, регистрации событий и синхронизации времени.

2.3. Мониторинг аномалий функционирования всех информационных специальных средств обеспечения информационной безопасности.

2.4. Проверка наличия несанкционированных действий работников ПФИЦ УрО РАН и авторизованных третьих лиц осуществляется по электронным журналам аудита информационных систем.

2.5. Необходимость получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать опасность таких уязвимостей и принимать соответствующие меры для рассмотрения связанного с ним риска.

2.6. Проверка журналов аудита и анализ данных по инцидентам информационной безопасности проводят на регулярной основе.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ О РЕАГИРОВАНИИ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1. Назначение и область действия

1.1. Настоящее Положение о реагировании на инциденты информационной безопасности (далее «Положение») определяет основные правила и требования по обеспечению информационной безопасности ПФИЦ УрО РАН от угроз, связанных с некорректным информированием об инцидентах или использованием информации о них.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Все пользователи информационных систем, услуг и ресурсов ПФИЦ УрО РАН должны сообщать о любых замеченных или подозреваемых недостатках безопасности в системах или услугах так оперативно, насколько это возможно.

2.2. Все пользователи должны быть осведомлены о своей обязанности сообщать ответственным лицам (см. раздел 3.2) и своему руководству об известных им или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

2.3. Пользователи должны знать способы информирования об известных или подозреваемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить и учет сообщений об инцидентах и принятие соответствующих мер.

2.4. Работникам ПФИЦ УрО РАН запрещается распространять предупреждения о вирусах и иных угрозах безопасности, полученные от третьих лиц. Эти предупреждения необходимо перенаправлять в адрес ответственных лиц (см. раздел 3.2).

2.5. В случае обнаружения пропажи информационных ресурсов или компонентов информационных систем ПФИЦ УрО РАН следует незамедлительно сообщить об этом своему непосредственному руководителю.

2.6. Расследование инцидентов (нарушений) информационной безопасности в центре осуществляется в порядке, определенном действующим законодательством РФ и внутренними документами ПФИЦ УрО РАН, и обязательно документируется.

2.7. ПФИЦ УрО РАН осуществляет сбор соответствующих показаний (свидетельств), которые могут быть использованы для подтверждения действий, направленных против лица либо ПФИЦ УрО РАН и (или) нарушающих его права, в порядке, определенном действующим законодательством.

2.8. Если инцидент ИБ может привести к судебному разбирательству против лица или организации, то информация о таком инциденте должна собираться, храниться и представляться согласно правилам оформления свидетельств, изложенными в соответствующих инструкциях.

2.9. Все инциденты ИБ должны быть идентифицированы, зафиксированы, доведены до соответствующих служб и решены (минимизированы негативные последствия).

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих следующие функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.

ПОЛОЖЕНИЕ О ФИЗИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ

1. Назначение и область действия

1.1. Настоящее Положение о физической защите информационных ресурсов (далее – «Положение») определяет основные правила и требования по обеспечению информационной безопасности ПФИЦ УрО РАН от угроз, связанных с физическим воздействием на информационные ресурсы ПФИЦ УрО РАН.

1.2. Соответствует требованиям Политики информационной безопасности ПФИЦ УрО РАН.

1.3. Распространяется на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН. Является обязательным для исполнения.

2. Основные требования

2.1. Работники ПФИЦ УрО РАН и лица, работающие по договорам, должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится, передается или обрабатывается информация ПФИЦ УрО РАН.

2.2. Оборудование, поддерживающее функционирование критических информационных систем, должно быть установлено в отдельных помещениях. Помещения должны быть доступны только уполномоченному персоналу и защищены от преднамеренного или случайного повреждения.

2.3. Руководители подразделений ПФИЦ УрО РАН, а также назначенные ответственные лица должны быть осведомлены обо всех местах установки и хранения компьютерного оборудования.

2.4. Все места установки и хранения компьютерного оборудования должны быть защищены от воздействия окружающей среды и обеспечить уровень физического доступа, соответствующий степени важности оборудования и хранящейся на нем информации.

2.5. Компьютерное оборудование ПФИЦ УрО РАН должно быть защищено от угроз, связанных с отказом и сбоями системы обеспечения.

2.6. Силовые и телекоммуникационные кабели сети, по которым передаются данные или поддерживаются информационные услуги, должны быть защищены от перехвата информации и повреждения.

2.7. Конфиденциальную информацию и оборудование либо программное обеспечение, предназначенное для обработки или защиты конфиденциальной информации, разрешается выносить за пределы территории ПФИЦ УрО РАН только на основании соответствующего разрешения.

2.8. Должен существовать процесс предоставления и блокирования физического доступа к серверным комнатам, к центрам обработки и хранения данных.

2.9. При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, должны учитываться риски, связанные с работой вне помещений ПФИЦ УрО РАН.

2.10. При передаче (списании) оборудования, все носители информации должны быть проверены на предмет полного уничтожения содержащейся на них важной (конфиденциальной) информации и программного обеспечения с целью предотвращения возможности восстановления этой информации.

3. Роли и ответственность

3.1. Ответственность за соблюдение данного Положения возлагается на всех работников ПФИЦ УрО РАН и третьих лиц, использующих информационные ресурсы и системы ПФИЦ УрО РАН.

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений ПФИЦ УрО РАН; работников, участвующих в реализации пропускного режима; работников, ответственных за администрирование сегментов информационной телекоммуникационной системы ПФИЦ УрО РАН; работников, выполняющих функции: администраторов информационных систем, администраторов локальной вычислительной сети, администраторов по обеспечению безопасности информации.