Национальный исследовательский центр
«Курчатовский институт»
Федеральное государственное бюджетное учреждение
«Петербургский институт ядерной физики им. Б.П. Константинова»

Политика информационной безопасности ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»

г. Москва
2023 г.

СОДЕРЖАНИЕ

1 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие сокращения:

ИБ – Информационная безопасность

ИС – Информационная система

СУИБ – Система управления информационной безопасностью

НТС ИТ – Научно-технический совет по информационным технологиям

2 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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

3 ОБЛАСТЬ ПРИМЕНЕНИЯ

3.1 Настоящая Политика информационной безопасности (далее – «Политика») предназначена для установления единых норм, правил и требований к системе управления информационной безопасностью ФГБУ «ПИЯФ» НИЦ «Курчатовский Институт» (далее – «Институт»).

3.2 Система обеспечения ИБ представляет собой совокупность нормативно-правовых, организационных, технических мер по обеспечению защищенности интересов Института в информационной сфере, а также субъектов информационных отношений.

3.3 Система управления ИБ является составной частью общей системы управления Института, обеспечивает поддержку и управление процессами обеспечения ИБ на всех этапах деятельности корпоративной информационной системы.

3.4 Институт разрабатывает и внедряет систему управления ИБ, отвечающую требованиям и рекомендациям нормативных документов Российской Федерации.

3.5 Основные цели внедрения системы управления ИБ Института:

3.5.1 Защита конфиденциальности информационных ресурсов ограниченного доступа;

3.5.2 Обеспечение непрерывного авторизованного доступа к информационным ресурсам Института для поддержки основной деятельности;

3.5.3 Защита целостности существенной информации для обеспечения требуемого качества работ и эффективности процесса принятий решений;

3.5.4 Установление четкой ответственности за управление и использование информационных ресурсов Института;

3.5.5 Введение обоснованной и согласованной системы контроля и процедур по защите информации в структурных подразделениях Института, в информационно-технологических системах и сетях;

3.5.6 Повышение осведомленности работников Института и их понимания рисков, связанных с информационными ресурсами Института, повышение их квалификации в области информационной безопасности.

3.6 Положения настоящей Политики распространяются на все виды информации в Институте, хранящейся либо передающейся любыми способами, в том числе информацию, зафиксированную на материальных носителях.

3.7 Положения настоящей Политики также распространяются на средства приема, обработки, передачи, хранения и защиты информации Института.

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

3.9 Область применения настоящей Политики распространяется на все

подразделения Института, в которых обрабатывается информация, не составляющая государственную тайну.

4 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 защитыинформации в государственных информационных системах».

Требования государственного регулятора в области информационной безопасности, указанные в письме в адрес ФГБУ «ПИЯФ» от 28.04.2014 г. № 48/286 «О направлении отчета о проведении КТМ ОЗ».

Концепция информационной безопасности ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» (Приказ от 08.04.2015 г. № 74).

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.

5 ОБЩИЕ ПОЛОЖЕНИЯ

5.1 Информация – важный и жизненно необходимый ресурс Института. Поэтому Институт защищает информацию так же надежно, как и любой другой ценный ресурс Института. Институт не сможет 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 Институтом и используемая для поддержки его законной деятельности, либо разработанная (созданная) работниками при выполнении служебных обязанностей, принадлежит Институту. Это право распространяется на информацию, передаваемую посредством голосовой, факсимильной и электронной связи с использованием аппаратуры Института, на приобретенное и разработанное программное обеспечение, на электронные почтовые ящики, а также на бумажные и электронные файлы (данные) работников, структурных подразделений, дочерних и контролируемых организаций.

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 её обработки, Институт применяет меры по организационной безопасности и физической защите, технические меры безопасности, в том числе контроль доступа, криптографические технологии и другие технологии защиты информации. При этом мероприятия по охране и защите являются достаточными, законными и отвечают требованиям Института 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 Институт, обязано поддерживать конфиденциальность и целостность деловой информации Института и защищать эту информацию от несанкционированного, незаконного или случайного раскрытия, искажения или уничтожения.

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

5.6 Знание и соблюдение требований настоящей Политики обязательно для всех работников Института и третьих лиц, использующих информационные ресурсы Института.

6 ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

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

6.2 Положения по ИБ являются приложениями к настоящей Политике.

6.3 Правила доступа к информационным ресурсам Института определены в «Положении о доступе к информационным ресурсам» (Приложение № 2).

6.4 Принятие новых Положений, а также пересмотр или отмена действующих Положений оформляется документально и утверждается приказом директора Института.

6.5 Актуализация Положений осуществляется при изменении законодательной или нормативной базы в области ИБ, а также при изменении внутренней ситуации в Институте.

7 ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

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

7.2 Основными задачами управления ИБ являются:

7.2.1 Анализ состояния ИБ Института;

7.2.2 Выбор и внедрение мер обеспечения ИБ, адекватных целям и задачам деятельности Института;

7.2.3 Контроль выполнения правил ИБ;

7.2.4 Документальное подтверждение предупреждающих и корректирующих мер обеспечения ИБ.

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

7.4 Институт 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 Институт возлагает на руководителей структурных подразделений. Руководители структурных подразделений Института должны осуществлять эффективную реализацию правил информационной безопасности, распределять ресурсы и ответственность и обеспечивать выполнение установленных требований безопасности работникамиподчиненного подразделения.

7.6 НТС ИТ Института предоставляет руководству Института экспертные оценки и рекомендации по вопросам обеспечения информационной безопасности.

8 РЕАЛИЗАЦИЯ

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

8.1 Структура и ответственность

8.1.1 Ответственное лицо, назначенное приказом директора Института, 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 Института осуществляют руководители этих подразделений. Они же несут ответственность за выполнение обязательств Положений по ИБ.

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

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

8.1.5 Все работники Института 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 Института или ее отдельных компонентов, несанкционированный доступ к информации либо нарушение

авторских и смежных прав в соответствии с нормативными актами Института и законодательством Российской Федерации.

8.2 Осведомленность и информирование

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

8.2.2 Перед началом работы в информационных системах Института работники получают у своего руководителя и знакомятся с «Инструкцией пользователя информационных систем ФГБУ «ПИЯФ» НИЦ «Курчатовский институт».

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 наинформационных стендах в помещениях Института.

8.3 Реагирование на инциденты безопасности

Для определения возможных сценариев восстановления информационной системы Института в чрезвычайных ситуациях, конкретизации технических средств и действий работников и структурных подразделений по локализации инцидентов ИБ должны быть разработаны планы восстановительных работ для важных информационных ресурсов.

9 КОНТРОЛЬ

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

9.2 Контроль за актуальностью Политики осуществляет ответственное лицо, назначенное приказом директора Института.

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

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

10 СОВЕРШЕНСТВОВАНИЕ

10.1 Для совершенствования системы управления ИБ в Институте выполняется систематический анализ и оценивание действующей ситуации 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 НТС ИТ Института с целью их оценки и выработки согласованных рекомендаций, направленных на формирование и реализацию корректирующих и превентивных действий по совершенствованию системы управления ИБ Института.

10.5 Рекомендации, принятые на заседании НТС ИТ, заносятся в протокол, который утверждается председателем НТС ИТ Института.

10.6 На основании утвержденного протокола НТС ИТ Института организует 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 Концепцией и Политикой информационной безопасности Института.

10.8 Нормативные и организационно-распорядительные документы по информационной безопасности утверждаются приказами по Институту и рассылаются руководству Института и руководителям подразделений.

10.9 Институт будет применять следующий системный подход к обеспечению исполнения требований и правил по информационной безопасности:

10.9.1 Настоящая Политика информационной безопасности ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» считается официально принятым документом после его утверждения приказом директора Института.

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 Институту, а также уточнены и дополнены распоряжениями по отдельному структурному подразделению.

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

Приложение № 1
к Политике информационной безопасности
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»

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 её передачи.

Владелец информационного ресурса – работник или структурное подразделение Института, распоряжающийся 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, устанавливаемыми 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 её инфраструктуры) от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или инфраструктуре (согласно Концепции ИБ Института).

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 **информационной безопасности Института** охватывает как процессы защиты, так и состояние защищенности

информации, информационной инфраструктуры и интересов Института в информационной сфере.

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

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

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

Информационные процессы – **п**роцессы 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 перегрузки;
- ошибки пользователей;
- несоблюдение политики или рекомендаций по ИБ;
- нарушение физических мер защиты;
- неконтролируемые изменения систем;
- 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 Института, используемая для автоматизации процессов обработки информации и управления, реализуемая средствами информационных технологий и организационными мерами.

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

Управление рисками ИБ Института – скоординированные действия по руководству и управлению Институтом 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.

Нарушитель 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, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.

Обеспечение ИБ Института – деятельность, направленная на устранение (нейтрализацию, парирование) внутренних и внешних угроз информационной безопасности Института 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 являются: 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 Института, 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 Институтом, 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 иресурсы (по ГОСТ Р 53114-2008).

Система обеспечения информационной безопасности – совокупность нормативно-правовых, организационных и технических мер по обеспечению защищенности интересов Института 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 документови 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 ее 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.

Ресурс 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 – **с**овокупность прав, привилегий и ограничений на использование ресурсов корпоративной информационной системы, предоставляемая работникам Института и третьим лицам для 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 обеспечивать неизменность информации в условиях её случайного и (или) преднамеренного искажения (разрушения).

Приложение № 2
к Политике информационной безопасности
ФГБУ «ПИЯФ» НИЦ «Курчатовский институт»

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 ФГБУ «ПИЯФ» НИЦ «Курчатовский институт» (далее – «Институт») от любых форм неавторизованного доступа, использования и раскрытия информации.

1.2 Соответствует требованиям Концепции и Политики информационной безопасности Института.

1.3 Распространяется на всех работников Института и третьих лиц, использующих информационные ресурсы и системы Института. 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 Института, в отношении которых Институт имеет права владения, распоряжения, пользования: данные (информация), технические средства, программные средства, услуги (сервисы) информационных систем.

2.3 Каждому пользователю сопоставляется учетная записьпользователя, присваиваются, по возможности, единые для различных объектов доступа Института атрибуты информационной безопасности: уникальный идентификатор, «секрет» аутентификации, права доступа – с учетом их

важности и ценности для деятельности Института.

2.4 В Институте 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 или 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 Института.

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 Института на отдельные логические и физические сетевые сегменты.

2.10 В Институте должны использоваться средства контроля над соблюдением правил доступа к объектам доступа.

2.11 Служебный доступ к объектам доступа Института, осуществляемый по внешним каналам связи, должен защищаться спримененим механизмов аутентификации и криптографической защитыинформации.

2.12 Доступ к общедоступным страницам веб-сайтов Института 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 проверяться на наличие уязвимостей и автоматически получать обновления безопасности.

2.14 Объекты доступа Института должны быть защищены отвнешних 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 определяются требования по управлению доступом к этим услугам.

2.16 При увольнении работника обеспечивается невозможность его доступа к объектам доступа Института.

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

2.17 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 Института. Разработка и утверждение этих документов производится вне настоящего Положения.

3 Роли и ответственность

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

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