Министерство науки и высшего образования
Российской Федерации
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ
БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ НАУКИ
ИНСТИТУТ СИСТЕМ ЭНЕРГЕТИКИ
им. Л.А. МЕЛЕНТЬЕВА
СИБИРСКОГО ОТДЕЛЕНИЯ
РОССИЙСКОЙ АКАДЕМИИ НАУК
(ИСЭМ СО РАН)

П Р И К А З

от "4" апреля 2024 г. г. Иркутск № 10

Об утверждении политики информационной безопасности и инструкции пользователя информационных систем ИСЭМ СО РАН

В целях принятия дальнейших мер по защите информации в ИСЭМ СО РАН (далее – Институт) в соответствии с Федеральным законом от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации приказываю:

1. Утвердить и ввести в действие Политику информационной безопасности ФГБУН «ИСЭМ СО РАН» (Приложение № 1).
2. Утвердить и ввести в действие Инструкцию пользователя информационных систем ФГБУН «ИСЭМ СО РАН» (Приложение № 2).
3. Руководство работами по внедрению и актуализации Политики информационной безопасности возложить на начальника научно-технического отдела информационных технологий и информационной безопасности Пальцева А.С.
4. Обязанности по контролю соблюдения требований Политики информационной безопасности возложить на сотрудников научно-технического отдела информационных технологий и информационной безопасности.
5. Контроль за исполнением настоящего приказа оставляю за собой.

Директор института
академик РАН В.А. Стенников

Приложение №1
к приказу №10 от "4" апреля 2024 г.

Политика информационной безопасности ФГБУН «Институт Систем Энергетики им. Л.А. Мелентьева СО РАН»

1. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие сокращения:

ИБ - Информационная безопасность
ИС - Информационная система
СУИБ - Система управления информационной безопасностью
НТО ИТИБ - Научно-технический отдел информационных технологий и информационной безопасности

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

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.

Аутентификация пользователя – процесс проверки пользователя системой для подтверждения того, что пользователь соответствует заявленному.

Безопасность информации (данных) - Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

Безопасность информационной технологии - Состояние защищенности информационной технологии, при котором обеспечиваются безопасность информации, для обработки которой она применяется, и информационная безопасность системы, в которой она реализована.

Блокирование информации (данных) - временное прекращение сбора, систематизации, накопления, использования, распространения информации.

Виртуальная частная сеть (VPN) - технология, позволяющая создавать безопасное подключение пользователя к сети, организованной между разными компьютерами.

Владелец информационного ресурса - сотрудник (или структурное подразделение) Института, распоряжающийся информационным ресурсом, в том числе определяющий порядок доступа к нему и его использования.

Вредоносное программное обеспечение (ВПО) - 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.

Идентификация риска - процесс обнаружения, распознавания и описания рисков.

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. 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.

Информационная инфраструктура - совокупность объектов информатизации, обеспечивающая доступ потребителей к информационным ресурсам.

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 (компьютерный инцидент) - непредвиденное или нежелательное событие, которое может нарушить деятельность Института в информационной сфере или информационную безопасность.

Источник угрозы безопасности - субъект, материальный объект или физическое явление, являющееся 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 информационная система Института, используемая для автоматизации процессов обработки информации и управления, реализуемая средствами информационных технологий и организационными мерами.

Локальная вычислительная сеть - объединение вычислительных устройств в единую информационную сеть с использованием средств проводной или беспроводной связи.

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.

Носитель ключевой информации – компактное устройство (чаще всего USB), которое служит для авторизации пользователя в сети или на локальном

компьютере, защиты электронной переписки, безопасного удаленного доступа к информационным ресурсам, а также надежного хранения персональных данных.

Обеспечение ИБ Института - деятельность, направленная на устранение (нейтрализацию, отражение) внутренних и внешних угроз информационной безопасности Института или на минимизацию ущерба от возможной реализации таких угроз.

Обеспечение целостности информации (данных) - способность средства вычислительной техники или информационной системы обеспечивать неизменность информации в условиях её случайного и (или) преднамеренного искажения (разрушения).

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.

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.

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.

Оценка риска - процесс, объединяющий идентификацию риска, анализ риска и их количественную оценку.

Политика - общее намерение и направление, официально выраженное руководством.

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 вредоносного программного обеспечения.

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. Применительно к ИБ, риск - сочетание вероятности нанесения ущерба и тяжести этого ущерба.

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.

Система обеспечения информационной безопасности - совокупность нормативно-правовых, организационных и технических мер по обеспечению защищенности интересов Института в информационной сфере.

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.

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.

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.

Третья сторона - лица или организация, которые признаны независимыми от участвующих сторон, по отношению к рассматриваемой проблеме.

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 иные несанкционированные действия при её обработке в информационных системах.

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.

Управление рисками ИБ Института - скоординированные действия по руководству и управлению Институтом в отношении рисков ИБ с целью их минимизации.

Уязвимость - слабость в средствах защиты информации, которую можно использовать для нарушения информационной безопасности системы или несанкционированного доступа к содержащейся в ней информации.

3. ОБЛАСТЬ ПРИМЕНЕНИЯ

3.1. Настоящая Политика информационной безопасности (далее - «Политика») предназначена для установления единых норм, правил и требований к

системе управления информационной безопасностью ФГБУН «Институт Систем энергетики им. Л.А. Мелентьева СО РАН» (далее - «Институт»).

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

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.

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 сотрудников Института и их понимания рисков, связанных с информационными ресурсами Института, повышение их квалификации в области ИБ.

3.6. Положения настоящей Политики распространяются на все виды информации в Институте, хранящейся либо передающейся любыми способами, в том числе на 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 сотрудникам Института, а также к любой третьей стороне, включая лиц, работающих по договорам гражданско-правового характера и командированных лиц, имеющих доступ к информационным ресурсам Института.

3.9. Область применения настоящей Политики распространяется на все подразделения Института.

4. НОРМАТИВНЫЕ ССЫЛКИ И ДОКУМЕНТЫ

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».

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

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 ресурс Института. Институт не сможет достичь своих уставных целей, если сотрудники не будут своевременно и в полном объеме получать информацию, необходимую для выполнения их обязанностей. Помимо этого, крайне важно минимизировать риски и ущерб, связанные с возможным раскрытием информации, её искажением и компрометацией.

5.2. Вся информация в любой форме, приобретенная или полученная Институтом и используемая для поддержки его деятельности, либо разработанная (созданная) сотрудниками при выполнении служебных обязанностей, принадлежит Институту. Это право распространяется на информацию, передаваемую посредством голосовой и электронной связи с использованием технических средств Института, на приобретенное и разработанное программное обеспечение, на электронные почтовые ящики, а также на бумажные и электронные файлы (данные) сотрудников и структурных подразделений.

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 организационные меры по безопасности, меры по физической защите, технические меры безопасности, в том числе контроль доступа, криптографические и другие технологии защиты информации. При этом вышеуказанные меры являются достаточными и законными. Настоящая Политика соответствует законодательству Российской Федерации, руководящим документам ФСБ и ФСТЭК России, а также внутренним документам в области безопасности.

5.4. Любое лицо, являющееся сотрудником Института, обязано поддерживать конфиденциальность и целостность информации Института и защищать эту информацию от несанкционированного, незаконного или случайного раскрытия, искажения или уничтожения.

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

5.6. Знание и соблюдение требований и правил настоящей Политики обязательно для всех сотрудников 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 Политики информационной безопасности Института в целях создания, развития и совершенствования общей системы защиты информации Института.

6.2. Положения по ИБ являются пунктами настоящей Политики.

6.3. Правила доступа к информационным ресурсам Института определены в «Положении о доступе к информационным ресурсам» (пункт 11).

6.4. Правила использования паролей определены в «Положении об использовании паролей» (пункт 12).

6.5. Программное обеспечение в Институте используется в соответствии с «Положением об использовании программного обеспечения» (пункт 13).

6.6. Правила пользования ресурсами сети Интернет в Институте указаны в «Положении об использовании сети интернет» (пункт 14).

6.7. Правила пользования электронной почтой Института указаны в «Положении об использовании электронной почты» (пункт 15).

6.8. Правила защиты от вредоносного программного обеспечения определены в «Положении о защите от вредоносного программного обеспечения» (пункт 16).

6.9. Правила использования средств беспроводного доступа приведены в «Положении об использовании средств беспроводного доступа» (пункт 17).

6.10. Правила использования мобильных устройств приведены в «Положении об использовании мобильных устройств» (пункт 18).

6.11. Правила и порядок организации рабочих мест определены в «Положении об организации рабочих мест» (пункт 19).

6.12. Общие правила технического обслуживания элементов информационных систем указаны в «Положении о техническом обслуживании» (пункт 20).

6.13. Правила классификации информационных ресурсов Института в целях обеспечения их защиты определены в «Положении о классификации информации» (пункт 21).

6.14. Инвентаризация информационных ресурсов и систем Института проводится в соответствии с «Положением об инвентаризации информационных ресурсов и систем» (пункт 22).

6.15. Мониторинг информационной безопасности в Институте выполняется в соответствии с «Положением о мониторинге событий информационной безопасности» (пункт 23).

6.16. Реагирование на инциденты ИБ в Институте осуществляется в соответствии с «Положением о реагировании на инциденты информационной безопасности» (пункт 24).

6.17. Меры по физической защите оборудования и данных предпринимаются в соответствии с «Положением о физической защите информационных ресурсов» (пункт 25).

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

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

7. ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

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

7.2. За управление ИБ в Институте отвечает Научно-технический отдел информационных технологий и информационной безопасности (НТО ИТИБ).

7.3. 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 мер обеспечения ИБ.

7.4. НТО ИТИБ осуществляет деятельность по управлению рисками, повышению осведомленности сотрудников Института в области ИБ и реагированию на инциденты ИБ.

7.5. Общая ответственность за защиту информации и информационных ресурсов Института возлагается на НТО ИТИБ. Вместе с тем, руководители структурных подразделений Института должны осуществлять эффективную реализацию правил информационной безопасности в своих подразделениях, обеспечивать выполнение установленных требований безопасности сотрудниками подразделения, а также нести ответственность за выполнение сотрудниками данных требований.

7.6. НТО ИТИБ предоставляет руководству Института оценки и рекомендации по вопросам обеспечения информационной безопасности.

8. РЕАЛИЗАЦИЯ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

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

8.1. Структура и ответственность

8.1.1. Руководитель НТО ИТИБ, назначенный 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 данных подразделений под кураторством руководителя НТО ИТИБ. Они же несут ответственность за выполнение сотрудниками подразделений требований настоящей Политики.

8.1.3. Ответственность сотрудников Института за надлежащее выполнение требований и правил ИБ указана в «Инструкции пользователя информационных систем ФГБУН «ИСЭМ СО РАН» (Приложение 2 к приказу о настоящей Политике).

8.1.4. Все сотрудники Института несут персональную 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 сотрудников Института по вопросам информационной безопасности.

8.2.2. Перед началом работы в информационных системах Института сотрудники получают у своего руководителя, либо от начальника НТО ИТИБ «Инструкцию пользователя информационных систем ФГБУН «ИСЭМ СО РАН» (Приложение 2 к приказу о настоящей Политике) и знакомятся с ней.

8.2.3. Доведение правил ИБ до сотрудников проводится: при приеме на работу; в ходе производственных совещаний, собраний, лекций и тренингов по информационной безопасности, проводимых НТО ИТИБ; с помощью электронной почты и других технических средств.

8.3. Реагирование на инциденты ИБ осуществляется в соответствии с «Положением о реагировании на инциденты информационной безопасности» (пункт 24 настоящей Политики).

9. КОНТРОЛЬ В ОБЛАСТИ ИБ

9.1. Контроль соблюдения требований настоящей Политики возлагается на ответственное лицо, назначенное приказом директора Института (Руководителя НТО ИТИБ). При необходимости контролирующие функции выполняют также сотрудники НТО ИТИБ.

9.2. Контроль за актуальностью Политики осуществляет руководитель НТО ИТИБ.

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, информационные системы и технические средства, а также средства защиты информации), а также сотрудники Института.

9.5. Контроль в области ИБ проводится в форме мониторинга ИБ, который выполняется в соответствии с «Положением о мониторинге событий информационной безопасности» (пункт 23 настоящей Политики).

10. СОВЕРШЕНСТВОВАНИЕ СИСТЕМЫ ИБ

10.1. Для совершенствования системы управления ИБ в Институте выполняется систематический анализ и оценка действующей ситуации в области информационной безопасности.

10.2. Анализ ИБ осуществляется на основе данных мониторинга в соответствии с «Положением о мониторинге событий ИБ» (пункт 23 настоящей Политики).

10.3. В ситуациях, требующих оперативного реагирования, работа ведется согласно «Положению о реагировании на инциденты ИБ» (пункт 24 настоящей Политики).

10.4. Обобщенные результаты анализа ИБ обсуждаются в НТО ИТИБ с целью их оценки и выработки рекомендаций, направленных на формирование и реализацию действий по совершенствованию системы управления ИБ Института.

10.5. На основании обсуждений и рекомендаций НТО ИТИБ организует подготовку нормативных и организационно-распорядительных документов (положений, инструкций, регламентов и других), направленных на совершенствование СУИБ.

10.6. Нормативные и организационно-распорядительные документы по информационной безопасности разрабатываются в строгом соответствии с Настоящей Политикой.

10.7. Нормативные и организационно-распорядительные документы по информационной безопасности утверждаются приказами по Институту.

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

10.8.1. Настоящая Политика информационной безопасности считается официально принятым документом после его утверждения приказом директора Института.

10.8.2. Все нормативные и организационно-распорядительные документы по информационной безопасности могут быть приняты, отменены и пересмотрены отдельными приказами по Институту.

10.8.3. Внутренние документы подразделений Института не должны противоречить 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.

11. ПОЛОЖЕНИЕ О ДОСТУПЕ К ИНФОРМАЦИОННЫМ РЕСУРСАМ

11.1. Назначение и область действия

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

11.1.2. Соответствует требованиям Политики информационной безопасности Института.

11.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

11.1.4. Является обязательным для исполнения.

11.2. Основные требования

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

11.2.2. 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.

11.2.3. В Институте могут применяться виды аутентификации, основанные на знании пользователем пароля (базовый вид аутентификации), а также на владении физическим носителем ключевой информации (смарт-карты, устройства контактной памяти, USB-ключи).

11.2.4. Пользователи уведомляются об обязанностях по обращению с носителями ключевой информации и сроках истечения их действия.

11.2.5. Категорически запрещен доступ к значимым ресурсам по принципу «Всем - Полный доступ». Запрещен также неавторизованный (анонимный, гостевой) доступ к любым ресурсам, кроме общедоступных страниц веб-сайта Института.

11.2.6. Управление доступом к сетевым информационным ресурсам и услугам производится, в том числе, путем разделения локальной вычислительной сети Института на отдельные логические и физические сетевые сегменты.

11.2.7. Служебный доступ к информационным ресурсам и объектам доступа Института, осуществляемый извне по внешним каналам связи, должен защищаться с применением механизмов аутентификации и криптографической защиты информации, а также с применением виртуальных частных сетей (VPN). Необходимость такого доступа обосновывается в служебных записках и заявлениях

сотрудников Института на имя руководителя НТО ИТИБ и утверждается руководителем НТО ИТИБ.

11.2.8. Доступ к общедоступным страницам веб-сайта Института не требует соблюдения требований раздела 11.2.7, достаточно обеспечить шифрование трафика.

11.2.9. Для снижения вероятности угроз несанкционированного доступа к информационным ресурсам Института, необходимо минимизировать число устройств, имеющих легальные “белые” внешние IP-адреса сети Интернет. Список оборудования, имеющего такие адреса, строго документируется в НТО ИТИБ и утверждается руководителем отдела. Данное оборудование должно постоянно проверяться на наличие уязвимостей и получать обновления безопасности.

11.2.10. Информационные ресурсы и объекты доступа Института должны быть защищены от внешних угроз из сети Интернет и из локальной сети межсетевыми экранами и штатными средствами защиты, входящими в состав операционной системы и приложений. Также на значимые ресурсы необходимо устанавливать дополнительные средства защиты информации (антивирус, средства обнаружения вторжений, средства контроля приложений и устройств и т.п.). Число открытых для доступа сервисов и ресурсов на данных объектах доступа должно быть минимально необходимым.

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

11.2.12. При увольнении сотрудника обеспечивается невозможность его доступа к объектам доступа Института.

11.2.13. При нарушении требований данного Положения доступ пользователя к информационным ресурсам может быть временно или постоянно заблокирован ответственными лицами (см. пункт 11.3.2).

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

11.3. Роли и ответственность

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

11.3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Института; руководителя и сотрудников НТО ИТИБ.

12. ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ПАРОЛЕЙ (ПАРОЛЬНОЙ ЗАЩИТЕ)

12.1. Назначение и область действия

12.1.1. Настоящее Положение об использовании паролей (далее - «Положение») определяет основные правила и требования по обеспечению информационной безопасности Института в области угроз, связанных с некорректным использованием средств аутентификации (паролей).

12.1.2. Соответствует требованиям Политики информационной безопасности Института.

12.1.3. Распространяется на всех сотрудников Института и третьих лиц, имеющих доступ или ответственных за предоставление доступа к любым информационным системам Института.

12.1.4. Является обязательным для исполнения.

12.2. Основные требования

12.2.1. Пароли пользователей (для доступа к электронной почте, компьютеру и т.д.) должны содержать не менее восьми символов (обязательно как минимум одну букву латинского алфавита в верхнем и нижнем регистре, одну цифру и один специальный символ типа ! @ # $ % ^ & * _ = и т.п.).

12.2.2. Административные пароли (пароли телекоммуникационного и сетевого оборудования, баз данных, информационных систем и т.д.) должны содержать не менее десяти символов (буквы латинского алфавита в верхнем и нижнем регистре, цифры и специальные символы типа ! @ # $ % ^ & * _ = и т.п.).

12.2.3. Пароль не должен совпадать с логином пользователя (наименованием учетной записи), содержать легко угадываемые слова и числа (имена, даты рождения, номера документов и т.п.), состоять только из букв или только из цифр, содержать словарные слова английского алфавита.

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

12.2.5. Запрещается передача паролей третьим лицам.

12.2.6. Запрещается запись и хранение паролей в местах, где они могут быть легко доступны и прочитаны (например, на клавиатуре и мониторе компьютера, на столе и т.д.).

12.2.7. Запрещается отправлять пароли в сообщениях электронной почты, SMS или через другие формы электронного обмена информацией, кроме специально оговоренных случаев (например, одноразовые пароли с ограниченным сроком действия и т.п.)

12.2.8. Доступ к общедоступным ресурсам Института, а также к страницам веб-сайта Института не требует парольной защиты.

12.2.9. В случае компрометации пароля (утраты, хищения, ввода пароля на мошеннических сайтах и т.п.), пользователь должен незамедлительно обратиться в НТО ИТИБ. Сотрудник НТО ИТИБ заменяет пароль пользователя новым паролем, который сообщает пользователю.

12.2.10. Учетные записи пользователей, чьи пароли не соответствуют требованиям настоящего Положения, могут быть заблокированы ответственными лицами (см. пункт 12.3.2).

12.3. Роли и ответственность

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

12.3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений Института. Ответственность за обеспечение технической возможности выполнения требований пунктов 12.2.1-12.2.9 и за соблюдение требований пунктов 12.2.1-12.2.10 возлагается на руководителя и сотрудников НТО ИТИБ.

13. ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

13.1. Назначение и область действия

13.1.1. Настоящее Положение об использовании программного обеспечения (далее - «Положение») определяет основные правила и требования по обеспечению информационной безопасности Института в области угроз, связанных с использованием программного обеспечения (далее - «ПО»).

13.1.2. Соответствует требованиям Политики информационной безопасности Института.

13.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

13.1.4. Является обязательным для исполнения.

13.2. Основные требования

13.2.1. В Институте разрешается использовать следующие виды ПО:

а) ПО, разработанное в Институте для обеспечения деятельности Института;

б) ПО, законно приобретенное или полученное Институтом на основании договорных или лицензионных соглашений с разработчиком либо правообладателем;

в) «свободное» ПО, распространяемое с открытым исходным кодом (Open Source) либо под свободными лицензиями;

г) «бесплатное» ПО, лицензия на которое явно допускает его безвозмездное использование в корпоративной среде.

13.2.2. Пользователям **ЗАПРЕЩЕНО:**

а) получать (приносить, скачивать), хранить, устанавливать и использовать нелицензионное программное обеспечение;

б) использовать программное и аппаратное обеспечение Института в неслужебных (личных) целях;

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

13.2.3. Пользователи могут самостоятельно устанавливать и обновлять необходимое для работы ПО на своих рабочих местах после согласования с отделом НТО ИТИБ. При этом каждый пользователь несет персональную ответственность за ПО, установленное на его рабочей станции.

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

13.2.5. Требования к представителям сторонних организаций, использующих в своей деятельности ПО Института, должны включаться в соответствующие договоры.

13.2.6. ПО, установленное или используемое в Институте в нарушение настоящего Положения, может быть заблокировано или удалено ответственными лицами (см. пункт 13.3.2).

13.3.2. Роли и ответственность

13.3.1. Ответственность за соблюдение требований пунктов 13.2.1-13.2.4 данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих в своей деятельности в Институте программное обеспечение.

13.3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений Института. Ответственность за обеспечение технической возможности выполнения требований пунктов 13.2.1-13.2.4 и за соблюдение требований пунктов 13.2.1-13.2.6 возлагается на руководителя и сотрудников НТО ИТИБ.

14. ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ СЕТИ ИНТЕРНЕТ

14.1. Назначение и область действия

14.1.1. Настоящее Положение об использовании сети Интернет (далее - «Положение») определяет основные правила и требования по обеспечению информационной безопасности Института в области угроз, связанных с воздействием программ из сети Интернет, а также веб-сайтов, разработанных или модифицированных для несанкционированного уничтожения, блокирования, модификации либо копирования информации, а также нарушения нормального функционирования элементов информационных систем Института.

14.1.2. Соответствует требованиям Политики информационной безопасности Института.

14.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института для доступа в сеть Интернет.

14.1.4. Является обязательным для исполнения.

14.2. Основные требования

14.2.1. Доступ сотрудника в сеть Интернет предоставляется на основании заявления сотрудника на имя руководителя НТО ИТИБ.

14.2.2. Доступ в сеть Интернет (беспроводной) для участников конференций, семинаров, иных проводимых в Институте мероприятий возможен только в помещениях, где проводятся данные мероприятия, с соблюдением Положения об использовании средств беспроводного доступа (пункт 17 Политики

информационной безопасности). Пароль для беспроводного доступа выдаётся участникам мероприятия сотрудником НТО ИТИБ.

14.2.3. Проводной доступ в сеть Интернет для участия сотрудников Института в конференциях и семинарах в удалённом режиме возможен в Конференц-зале Института, малом Конференц-зале Института, либо в аудитории 310 (музей ИСЭМ СО РАН).

14.2.4. В случае, если сотруднику Института необходим доступ в сеть Интернет с рабочего места через технологию VPN (для участия в конференциях или иных служебных обязанностей), сотрудник должен написать заявление на имя руководителя НТО ИТИБ с указанием цели использования VPN и срока, на который ему необходим данный доступ. Заявление утверждается руководителем НТО ИТИБ.

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

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

14.2.7. 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.

14.2.8. В Институте проводится мониторинг информации, принимаемой и передаваемой посредством сети Интернет с использованием информационных систем Института.

14.2.9. При увольнении сотрудника его доступ к сети Интернет блокируется ответственным лицом (сотрудником НТО ИТИБ) после получения информации об увольнении от Отдела кадров Института.

14.2.10. Лица, ответственные за обеспечение и контроль доступа в сеть Интернет (см. раздел 14.3.2), могут заблокировать доступ в сеть Интернет для сотрудников, допустивших нарушения данного Положения.

14.3. Роли и ответственность

14.3.1. Ответственность за соблюдение данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих в своей деятельности информационные системы Института для доступа в сеть Интернет.

14.3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений Института. Ответственность за обеспечение и контроль доступа в сеть Интернет возлагается на руководителя и сотрудников НТО ИТИБ.

15. ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ ЭЛЕКТРОННОЙ ПОЧТЫ

15.1. Назначение и область действия

15.1.1. 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 Института, передаваемой и принимаемой посредством электронной почты.

15.1.2. Соответствует требованиям Политики информационной безопасности Института.

15.1.3. Распространяется на всех сотрудников Института и третьих лиц, взаимодействующих с Институтом посредством электронной почты либо использующих средства электронной почты Института.

15.1.4. Является обязательным для исполнения.

15.2. Основные требования

15.2.1. Доступ сотрудника к электронной почте Института предоставляется на основании заявления сотрудника на имя руководителя НТО ИТИБ.

15.2.2. Регистрация или смена адреса электронной почты для сотрудника осуществляется ответственным лицом (сотрудником НТО ИТИБ) после подписания руководителем НТО ИТИБ заявления на регистрацию или изменение адреса электронной почты.

15.2.3. Пароль к электронной почте должен содержать не менее 8 символов (как минимум одну букву латинского алфавита в верхнем регистре, одну цифру и один специальный символ типа ! @ # $ % ^ & * _ = и т.п.).

15.2.4. Все входящие и исходящие сообщения электронной почты должны проверяться на наличие ВПО.

15.2.5. Доступ к электронной почте Института возможен как из внутренней сети Института, так и извне (по адресу https://mail.isem.irk.ru).

15.2.6. Сотрудникам Института категорически запрещается вводить пароль от своей электронной почты куда-либо, кроме почтового приложения, установленного на рабочем месте, и страницы по адресу https://mail.isem.irk.ru. Сотрудники несут персональную ответственность за сохранность пароля от электронной почты.

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

15.2.8. Запрещена отправка пользователями и пересылка почтовыми серверами Института исполняемых, служебных и системных файлов, модулей и компонентов операционных систем и приложений.

15.2.9. Все факты отправки и приема электронных сообщений в Институте фиксируются.

15.2.10. При увольнении сотрудника доступ к его электронной почте блокируется. Удаление адреса и содержимого электронной почты уволенного

сотрудника производится ответственным лицом (сотрудником НТО ИТИБ) после получения информации об увольнении сотрудника от Отдела кадров Института.

15.2.11. При нарушении указанных в данном Положении правил работы с электронной почтой доступ сотрудника к электронной почте может быть временно приостановлен или заблокирован ответственными лицами (см. раздел 15.3.2) до устранения нарушения.

15.3. Роли и ответственность

15.3.1. Ответственность за соблюдение данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих информационные системы электронной почты Института.

15.3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений Института. Ответственность за обеспечение и контроль доступа к электронной почте возлагается на руководителя и сотрудников НТО ИТИБ.

16. ПОЛОЖЕНИЕ О ЗАЩИТЕ ОТ ВРЕДОНОСНОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

16.1. Назначение и область действия

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

16.1.2. Соответствует требованиям Политики информационной безопасности Института.

16.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

16.1.4. Является обязательным для исполнения.

16.2. Основные требования

16.2.1. Средства защиты от ВПО должны быть установлены, настроены и активированы на всех допускающих такую установку программно-технических средствах до начала их работы с информационными системами Института.

16.2.2. Средства защиты от ВПО должны регулярно получать обновления антивирусных баз из доверенных источников.

16.2.3. Контролю на предмет обнаружения ВПО должна подвергаться вся информация, создаваемая и (или) обрабатываемая программно-техническими средствами в Институте, а также принимаемая и (или) передаваемая с помощью машинных носителей (жёсткие диски, флэш-накопители) или средств телекоммуникаций (электронная почта, Интернет).

16.2.4. В соответствии с «Положением об использовании программного обеспечения», в Институте разрешается использовать только лицензионные, свободные или бесплатные средства защиты от ВПО.

16.2.5. Программно-технические средства (компьютеры, серверы и т.д.), допускающие установку средств защиты от ВПО, но не имеющие таковых, могут быть временно или постоянно отключены от информационных систем и локальной вычислительной сети Института ответственными лицами (см. раздел 16.3.2) при расследовании угроз безопасности, вирусных и иных атак, а также при расследовании компьютерных инцидентов.

16.3. Роли и ответственность

16.3.1. Ответственность за соблюдение требований пунктов 16.2.1-16.2.4 данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

16.3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений Института. Ответственность за обеспечение технической возможности выполнения требований пунктов 16.2.1-16.2.4 и за соблюдение требований пунктов 16.2.1-16.2.5 возлагается на руководителя и сотрудников НТО ИТИБ.

17. ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ СРЕДСТВ БЕСПРОВОДНОГО ДОСТУПА

17.1. Назначение и область действия

17.1.1. Настоящее Положение об использовании средств беспроводного доступа (далее - «Положение») определяет основные правила и требования по обеспечению информационной безопасности при эксплуатации беспроводных сетей в Институте.

17.1.2. Соответствует требованиям Политики информационной безопасности Института.

17.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

17.1.4. Является обязательным для исполнения.

17.2. Основные требования

17.2.1. Беспроводной доступ к информационным системам и ресурсам Института, а также к сети Интернет для сотрудников Института разрешается только при письменном заявлении сотрудника на имя руководителя НТО ИТИБ с указанием цели использования беспроводного доступа и срока, на который ему необходим данный доступ. Заявление утверждается руководителем НТО ИТИБ. Доступ осуществляется при соблюдении всех требований безопасности.

17.2.2. В случае использования сотрудником Института оборудования для беспроводного доступа, установленного в его рабочем помещении, сотрудник обязан написать заявление на имя руководителя НТО ИТИБ с указанием цели использования оборудования и срока, на который данное оборудование необходимо

задействовать, а также с принятием полной ответственности за свои действия или бездействие на данном оборудовании на себя. Заявление утверждается руководителем НТО ИТИБ.

17.2.3. Беспроводной доступ для участников конференций, семинаров, других мероприятий Института разрешается исключительно для выхода в сеть Интернет.

17.2.4. Логин и пароль для беспроводного доступа выдаются участникам мероприятий в соответствии с Положением об использовании паролей.

17.2.5. Беспроводной доступ осуществляется с использованием двух частотных диапазонов: 2,4 и 5,0 ГГц; регистрацией подключенных устройств по MAC-адресу с возможностью блокировки и предотвращения несанкционированного доступа; с поддержкой протокола шифрования WPA2.

17.3. Роли и ответственность

17.3.1. Ответственность за соблюдение данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих беспроводные средства передачи данных.

17.3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Института, руководителя и сотрудников НТО ИТИБ.

18. ПОЛОЖЕНИЕ ОБ ИСПОЛЬЗОВАНИИ МОБИЛЬНЫХ УСТРОЙСТВ

18.1. Назначение и область действия

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

18.1.2. Соответствует требованиям Политики информационной безопасности Института.

18.1.3. Распространяется на всех сотрудников Института и третьих лиц, взаимодействующих с Институтом и использующих его информационные ресурсы и системы.

18.1.4. Является обязательным для исполнения.

18.2. Основные требования

18.2.1. Порядок вноса в здание Института и выноса из него мобильных устройств обработки информации регламентируется внутренними документами Института.

18.2.2. Не допускается использование мобильных устройств обработки информации для осуществления звуковой и видеозаписи или ретрансляции переговоров и совещаний по вопросам, затрагивающим конфиденциальную информацию Института.

18.2.3. Сотрудники, осуществляющие эксплуатацию мобильных устройств обработки информации для хранения и обработки конфиденциальной информации Института, обязаны:

1) знать и соблюдать требования локальных нормативных актов Института по обеспечению информационной безопасности и инструкций по эксплуатации средств защиты информации;

2) использовать все доступные защитные механизмы для предотвращения доступа к конфиденциальной информации Института посторонних лиц;

3) не хранить конфиденциальную информацию Института в открытом виде вне сеансов работы с ней, а также во время соединения с другими информационными сетями;

4) не допускать передачу конфиденциальной информации Института по открытым каналам связи без принятия мер по ее криптографической защите;

5) своевременно информировать руководство и ответственных лиц (см. раздел 18.3.2) о фактах утечки конфиденциальной информации Института, утраты мобильных средств вычислительной техники и т.д.;

6) при прекращении использования мобильного средства обработки информации или при передаче его другому лицу - обеспечить уничтожение содержащейся в нем конфиденциальной информации Института.

18.3. Роли и ответственность

18.3.1. Ответственность за соблюдение данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих мобильные устройства обработки информации для работы с информационными ресурсами и системами Института.

18.3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Института; сотрудников, участвующих в реализации пропускного режима; руководителя и сотрудников НТО ИТИБ.

19. ПОЛОЖЕНИЕ ОБ ОРГАНИЗАЦИИ РАБОЧИХ МЕСТ

19.1. Назначение и область действия

19.1.1. Настоящее Положение об организации рабочих мест (далее - «Положение») определяет процесс организации рабочих мест для безопасного выполнения трудовых обязанностей сотрудниками Института.

19.1.2. Соответствует требованиям Политики информационной безопасности Института.

19.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

19.1.4. Является обязательным для исполнения.

19.2. Основные требования

19.2.1. При приеме на работу, при смене рабочего места, руководитель подразделения оформляет заявку на организацию рабочего места пользователя с указанием потребностей и направляет ее руководителю НТО ИТИБ.

19.2.2. Выполнение заявки на обеспечение или изменение доступа пользователя включает в себя назначение прав доступа к сетевым ресурсам локальной сети, сети Интернет, электронной почте Института, программному обеспечению, базам данных, телефонной связи и т.п.

19.2.3. При приёме на работу сотрудник обязан ознакомиться с Политикой информационной безопасности Института и всеми её положениями, а также с Инструкцией пользователя информационных систем Института, и расписаться в листе ознакомления, тем самым подтверждая ответственность за своё рабочее место.

19.2.4. С целью снижения рисков вследствие возможной недостаточной компьютерной грамотности нового сотрудника, его первый рабочий сеанс может производиться под контролем руководителя или ответственного лица.

19.2.5. В случае необходимости закрытия доступа пользователя к информационным ресурсам, руководитель подразделения заранее направляет заявку в адрес руководителя НТО ИТИБ. На основании этой заявки в течение двух рабочих дней блокируется доступ к сетевым ресурсам, информационным системам, электронной почте, сети Интернет и т.п. Такие же действия проводятся в случае увольнения сотрудника из Института.

19.2.6. В случае возможности ознакомления посторонним лицом с конфиденциальной информацией, предоставленной на экране компьютера или бумажном носителе в присутствии сотрудника Института, последний должен предпринять необходимые меры по предотвращению такого ознакомления.

19.2.7. 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.

19.2.8. Пользователям запрещается без согласования с руководством и с НТО ИТИБ использовать на рабочих местах оборудование и программное обеспечение, которые не нужны им для выполнения своих трудовых обязанностей, а также которые не принадлежат Институту на правах собственности, аренды, пользования, либо в отношении которых Институт не обладает иными (в том числе неисключительными) правами.

19.3. Роли и ответственность

19.3.1. Ответственность за соблюдение данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих информационные ресурсы Института.

19.3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Института, руководителя и сотрудников НТО ИТИБ.

20. ПОЛОЖЕНИЕ О ТЕХНИЧЕСКОМ ОБСЛУЖИВАНИИ

20.1. Назначение и область действия

20.1.1. Настоящее Положение о техническом обслуживании (далее - «Положение») определяет основные правила и требования по обеспечению

информационной безопасности Института от угроз, связанных с нарушением деятельности института из-за неисправностей оборудования, кабельных линий и т.п.

20.1.2. Соответствует требованиям Политики информационной безопасности Института.

20.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

20.1.4. Является обязательным для исполнения.

20.2. Основные требования

20.2.1. Техническое обслуживание и ремонт оборудования и кабельных линий (электропитания и телекоммуникации) производится только уполномоченными на это сотрудниками (персоналом соответствующих подразделений и обслуживающим персоналом) и документируется.

20.2.2. Техническое обслуживание оборудования и кабельных линий проводится регулярно.

20.2.3. 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, поддерживающее критические рабочие процессы, рекомендуется заменять резервным.

20.2.4. Все устройства хранения информации перед списанием или утилизацией проверяются на наличие конфиденциальной информации. При наличии таковой, они списываются или утилизируются по акту способом, гарантирующим невозможность восстановления хранящейся на них информации.

20.2.5. Выявленные в процессе технического обслуживания отклонения и неисправности регистрируются и устраняются немедленно либо (при необходимости) заносятся в планы по ремонту и обслуживанию.

20.3. Роли и ответственность

20.3.1. Ответственность за соблюдение данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих информационные ресурсы Института.

20.3.2. Ответственность за реализацию данного Положения возлагается на руководителей подразделений Института, руководителя и сотрудников НТО ИТИБ, руководителя и сотрудников службы главного инженера.

21. ПОЛОЖЕНИЕ О КЛАССИФИКАЦИИ ИНФОРМАЦИИ

21.1. Назначение и область действия

21.1.1. Настоящее Положение о классификации информации (далее - «Положение») определяет основные правила и требования по классификации информационных Института с точки зрения их ценности (важности) и критичности для деятельности Института в целях обеспечения адекватного уровня их защиты.

21.1.2. Соответствует требованиям Политики информационной безопасности Института.

21.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

21.1.4. Является обязательным для исполнения.

21.2. Основные требования

21.2.1. Для обеспечения уровней защиты информационных ресурсов в Институте, они классифицируются в соответствии со степенью важности содержащейся в них информации.

21.2.2. Информационные ресурсы Института классифицируются в соответствии со следующими тремя категориями:

I - содержит **конфиденциальные** сведения (особые 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).

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

21.2.4. В Институте информация категории I (конфиденциальная) подразделяется на:

- информацию, составляющую служебную и коммерческую тайну;
- персональные данные, защита которых организуется в соответствии с требованиями законодательства РФ.

21.2.5. Конфиденциальная информация, составляющая служебную и коммерческую тайну:

- не подлежит передаче по открытым каналам передачи данных и в открытой переписке без принятия мер защиты;
- не сообщается в личных и деловых переговорах по открытым каналам связи.

21.2.6. Использование персональных данных в деятельности Института производится только с согласия субъекта персональных данных. Порядок использования персональных данных определяется соответствующими внутренними документами, политиками и регламентами Института, разработка и утверждение которых производится вне настоящего Положения.

21.3. Роли и ответственность

21.3.1. Ответственность за соблюдение данного Положения возлагается на всех сотрудников Института и третьих лиц, использующих информационные ресурсы Института.

21.3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Института, руководителя и сотрудников НТО ИТИБ, руководителя первого отдела, ответственного за обработку персональных данных в Институте.

22. ПОЛОЖЕНИЕ ОБ ИНВЕНТАРИЗАЦИИ ИНФОРМАЦИОННЫХ РЕСУРСОВ И СИСТЕМ

22.1 Назначение и область действия

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

22.1.2. Соответствует требованиям Политики информационной безопасности Института.

22.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

22.1.4. Является обязательным для исполнения.

22.2. Основные требования

22.2.1. Все информационные ресурсы и системы Института подлежат инвентаризации с документированием результатов в соответствующем реестре.

22.2.2. Инвентаризации подлежат следующие типы информационных ресурсов, а также технических и программных средств: компьютерное оборудование, аппаратура связи, коммутационное и маршрутизационное оборудование, технические средства обеспечения ИБ, копировальные и печатающие устройства, проекционное оборудование, носители информации, установки электроснабжения, кондиционирования воздуха и т.д.; программные средства обеспечения ИБ.

22.2.3. В реестрах информационных ресурсов и систем, технических и программных средств отражаются следующие атрибуты: наименование, подразделение, ответственное лицо, местоположение, категория информационного ресурса.

22.2.4. Актуальность реестра обеспечивается на основе непрерывного процесса его поддержки.

22.3. Роли и ответственность

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

22.3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Института, руководителя и сотрудников НТО ИТИБ, лиц, ответственных за инвентаризацию в Институте.

23. ПОЛОЖЕНИЕ О МОНИТОРИНГЕ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

23.1. Назначение и область действия

23.1.1. 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 Института.

23.1.2. Соответствует требованиям Политики информационной безопасности Института.

23.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

23.1.4. Является обязательным для исполнения.

23.2. Основные требования

23.2.1. Мониторинг событий информационной безопасности проводится с целью выявления нецелевого использования средств обработки информации пользователями, несанкционированных действий сотрудников и третьих лиц в информационных системах Института, оперативного реагирования на инциденты информационной безопасности, сбора данных и проведения служебных расследований.

23.2.2. Для мониторинга событий информационной безопасности используются специализированные средства и штатные (входящие в состав информационных систем) средства контроля доступа, регистрации событий и т.д.

23.2.3. Мониторинг функционирования всех информационных систем Института реализуется с использованием специальных средств обеспечения информационной безопасности.

23.2.4. Проверка наличия несанкционированных действий сотрудников Института и третьих лиц осуществляется по электронным журналам аудита информационных систем, системным журналам, логам и т.п.

23.2.5. Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать опасность таких уязвимостей и принимать соответствующие меры для оценки рисков и устранения данных уязвимостей.

23.2.6. Проверка журналов аудита, системных журналов информационных систем и анализ данных по инцидентам информационной безопасности проводятся на регулярной основе.

23.3. Роли и ответственность

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

3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Института; руководителя и сотрудников НТО ИТИБ.

24. ПОЛОЖЕНИЕ О РЕАГИРОВАНИИ НА ИНЦИДЕНТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

24.1. Назначение и область действия

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

24.1.2. Соответствует требованиям Политики информационной безопасности Института.

24.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

24.1.4. Является обязательным для исполнения.

24.2 Основные требования

24.2.1. Все пользователи информационных систем и ресурсов Института должны оперативно сообщать ответственным лицам (см. пункт 24.3.2) о любых замеченных недостатках безопасности в системах или ресурсах, а также об известных им нарушениях и инцидентах информационной безопасности.

24.2.2. Пользователи информационных систем и ресурсов Института должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты, сети Интернет и др. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

24.2.3. Сотрудникам Института запрещается распространять предупреждения о вирусах и иных угрозах информационной безопасности, полученные от третьих лиц. Эти предупреждения необходимо перенаправлять в адрес ответственных лиц (см. пункт 24.3.2).

24.2.4. Расследование инцидентов информационной безопасности в Институте осуществляется в порядке, определенном действующим законодательством РФ и внутренними документами Института, в том числе Политикой информационной безопасности, и обязательно документируется.

24.2.5. Институт осуществляет сбор соответствующих показаний (свидетельств), которые могут быть использованы для подтверждения действий, направленных против Института и (или) нарушающих его права, в порядке, определенном действующим законодательством.

24.2.6. Если инцидент информационной безопасности может привести к судебному разбирательству против лица или организации, то информация о таком инциденте должна собираться, храниться и предоставляться согласно правилам, изложенным в соответствующих инструкциях.

24.2.7. Все инциденты информационной безопасности должны быть идентифицированы, зафиксированы, доведены до соответствующих служб и решены (минимизированы негативные последствия). Виновные в инцидентах должны быть установлены и привлечены к ответственности.

24.3. Роли и ответственность

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

24.3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Института; руководителя и сотрудников НТО ИТИБ.

25. ПОЛОЖЕНИЕ О ФИЗИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИОННЫХ РЕСУРСОВ

25.1. Назначение и область действия

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

25.1.2. Соответствует требованиям Политики информационной безопасности Института.

25.1.3. Распространяется на всех сотрудников Института и третьих лиц, использующих информационные ресурсы и системы Института.

25.1.4. Является обязательным для исполнения.

25.2. Основные требования

25.2.1. Сотрудники Института и третьи лица, использующие информационные ресурсы и системы Института, должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранится, передаётся или обрабатывается информация.

25.2.2. Доступ в Институт сотрудников и третьих лиц осуществляется при помощи системы контроля и управления доступом (СКУД), исключающей несанкционированное проникновение в помещения Института. Порядок и регламент использования СКУД определяется соответствующими внутренними документами, разработка и утверждение которых производится вне настоящего Положения.

25.2.3. Оборудование, поддерживающее функционирование критичных информационных систем, а также серверное оборудование, должно быть установлено в отдельных помещениях. Такие помещения должны быть доступны только уполномоченному персоналу и защищены от преднамеренного или случайного повреждения.

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

25.2.5. Компьютерное оборудование Института должно быть защищено от угроз, связанных с отказами и сбоями систем обеспечения.

25.2.6. Силовые и телекоммуникационные кабельные сети, по которым передаются данные, должны быть защищены от перехвата информации и повреждения.

25.2.7. Конфиденциальную информацию и оборудование либо программное обеспечение, предназначенное для обработки или защиты конфиденциальной информации, разрешается выносить за пределы Института только на основании соответствующего разрешения.

25.2.8. Должен существовать процесс предоставления и блокирования физического доступа к серверным помещениям, а также помещениям, где обрабатываются персональные данные.

25.2.9. При 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.

25.3. Роли и ответственность

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

25.3.2. Ответственность за реализацию данного Положения возлагается на: руководителей подразделений Института; руководителя и сотрудников НТО ИТИБ, сотрудников, участвующих в реализации пропускного режима.

Приложение №2
к приказу №_10_ от "_4_" _апреля_ 2024 г.

Инструкция пользователя информационных систем ФГБУН «Институт Систем Энергетики им. Л.А. Мелентьева СО РАН»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1. Инструкция пользователя информационных систем (далее - «Инструкция») определяет общие правила работы в информационных системах и сетях ФГБУН «Институт систем энергетики им. Л.А. Мелентьева СО РАН» (далее - «Институт»).

1.2. Настоящая Инструкция разработана в соответствии с требованиями Политики информационной безопасности Института. Сокращения, термины и определения, используемые в настоящей Инструкции, соответствуют Политике информационной безопасности Института.

1.3. Пользователями являются все сотрудники Института и третьи лица, имеющие доступ к информационным ресурсам и информационным системам (вычислительному и сетевому оборудованию, аппаратным средствам, программному обеспечению, данным и средствам их защиты) Института.

1.4. Пользователь в своей работе руководствуется настоящей Инструкцией, должностной инструкцией, Положением о своем подразделении, Политикой информационной безопасности Института, Уставом Института, а также нормативными и законодательными актами Российской Федерации.

1.5. Методическое руководство работой пользователя в информационных системах и сетях Института осуществляет его непосредственный руководитель, а также руководитель и сотрудники НТО ИТИБ.

2. ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЯ

2.1. Знать и выполнять требования законодательных актов Российской Федерации, настоящей Инструкции, Политики информационной безопасности и других внутренних документов Института, регламентирующих правила работы в информационных системах.

2.2. Выполнять на рабочем месте с использованием средств вычислительной техники только те действия, которые определены должностной инструкцией, служебными либо договорными обязанностями.

2.3. Использовать информационные ресурсы и системы Института только для выполнения порученных работ, а также исполнения должностных либо договорных обязанностей.

2.4. При прекращении трудовых отношений все средства вычислительной техники, а также материальные носители, содержащие служебную информацию (usb-накопители, магнитные и оптические диски и т.д.) - передать непосредственному руководителю в надлежащем состоянии.

3. ПРАВА ПОЛЬЗОВАТЕЛЯ

3.1. Использовать информационные ресурсы и системы Института, сеть Интернет, электронную почту для выполнения должностных обязанностей.

3.2. Направлять своему руководителю и руководителю НТО ИТИБ обоснованные предложения по приобретению и установке, а также модернизации программного и аппаратного обеспечения.

3.3. Получать от своего руководителя и сотрудников НТО ИТИБ инструктаж и консультации по правилам работы с информационными ресурсами, системами, сетью Интернет, электронной почтой и т.д.

3.4. Обращаться за помощью и консультациями в НТО ИТИБ по адресам электронной почты: **admin@isem.irk.ru , paltsev@isem.irk.ru.**

4. ПРАВИЛА И ОГРАНИЧЕНИЯ

Пользователю ЗАПРЕЩАЕТСЯ:

4.1. Нарушать установленные в Институте правила работы в информационных системах и сетях.

4.2. Получать (приносить, скачивать), хранить, устанавливать и использовать программное обеспечение, которое не требуется для выполнения должностных обязанностей.

4.3. Использовать программное и аппаратное обеспечение Института в неслужебных (личных) целях.

4.4. Оставлять свое рабочее место, предварительно не заблокировав рабочий сеанс и не предприняв соответствующих мер по защите информации на физических носителях.

4.5. Без согласования с НТО ИТИБ изменять состав и конфигурацию используемых программных и аппаратных средств, устанавливать и модифицировать программное и аппаратное обеспечение.

4.6. Выполнять действия, направленные на получение несанкционированного доступа к информационным системам, компьютерам, серверам и сетям Института, а также к ресурсам сети Интернет.

4.7. Изменять параметры средств защиты информации (в том числе настройки брандмауэра и средств антивирусной защиты), а также прекращать их работу.

4.8. Использовать нерегламентированные (не относящиеся к работе, не разрешенные) программы и ресурсы: создающие избыточную нагрузку на сеть (игры, музыка, фильмы, P2P-клиенты), средства удаленного администрирования и т.д.

4.9. Без согласования с НТО ИТИБ создавать сетевые ресурсы совместного использования (папки и файлы общего доступа). Изменять содержимое сетевых ресурсов или права доступа к ним без разрешения их владельцев. Предоставлять права к любым ресурсам вида: «полный доступ для всех». Разрешать неавторизованный (анонимный, гостевой) доступ к сетевым ресурсам с правом на запись (изменение) содержимого.

4.10. В случае возникновения неисправностей в вычислительном или сетевом оборудовании Института - самостоятельно их устранять, не поставив в известность

непосредственного руководителя, а также руководителя или сотрудников НТО ИТИБ.

4.11. Препятствовать должностным лицам и ответственным сотрудникам Института при проведении проверок и служебных расследований, связанных с обеспечением информационной безопасности.

4.12. Удалять или изменять программы и файлы со служебными данными и иной важной информацией.

4.13. Использовать недокументированные свойства и ошибки в программном обеспечении или в настройках средств защиты информации, которые могут привести к возникновению внештатной ситуации или к компьютерному инциденту.

4.14. Без согласования с руководителем НТО ИТИБ подключать к сетям Института личные средства вычислительной техники, мобильные и сетевые устройства, а также изменять IP-адреса, MAC-адреса и иные сетевые настройки любого оборудования.

4.15. Несанкционированно распространять конфиденциальную информацию, содержащую персональные данные, служебную или коммерческую тайну.

4.16. Распространять и получать материалы, противоречащие законодательству Российской Федерации и внутренним правилам Института.

5. ПАРОЛИ

5.1. Общие требования к паролям

5.1.1. Минимальная длина пароля (для компьютера, электронной почты и т.п.): восемь символов.

5.1.2. Минимальное требование к составу пароля: как минимум одна буква латинского алфавита в верхнем и нижнем регистре, одна цифра и один специальный символ типа ! @ # $ % ^ & * _ = и т.п.

5.1.3. Нельзя использовать повторно ранее использованные пароли.

5.1.4. Пароль не должен совпадать с именем учетной записи (логином) и содержать легко угадываемые слова и числа (имена, даты рождения и т.п.), общепринятые сокращения, номера документов и иную информацию о пользователе, доступную третьим лицам.

5.1.5. Нельзя использовать в качестве пароля один повторяющийся символ либо повторяющуюся комбинацию из нескольких символов.

5.1.6. Нельзя использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (123456, qwerty и т.п.).

5.2. Правила использования паролей

5.2.1. Пользователю **ЗАПРЕЩАЕТСЯ:**

- сообщать свой пароль третьим лицам;
- предоставлять третьим лицам доступ к своей рабочей станции, информационным системам, электронной почте и т.п. под своей учетной записью и паролем;
- записывать и хранить пароли в легкодоступных местах: в ящике стола, на мониторе, на листах бумаги, на клавиатуре и т.д.

5.2.2. Пользователь **ОБЯЗАН:**

- при вводе пароля - исключить возможность его считывания посторонними лицами или техническими средствами;
- немедленно сообщать руководителю и в НТО ИТИБ об утере, утечке, несанкционированном изменении пароля.

5.2.3. Внеплановая замена или удаление пароля пользователя производится в следующих случаях:

- при подозрении на компрометацию пароля;
- при прекращении полномочий (увольнение, смена обязанностей);
- по указанию руководителя или сотрудников НТО ИТИБ.

5.2.4. При увольнении или смене обязанностей пользователя, имеющего, кроме своей учетной записи, доступ к другим ресурсам (сетевое оборудование, серверы, административные учетные записи и т.п.) - производится также внеплановая смена паролей к этим ресурсам.

6. АНТИВИРУСНАЯ ЗАЩИТА

6.1. Пользователь **ОБЯЗАН** производить антивирусную проверку всех файлов, полученных им любым способом и из любого места.

6.2. При подозрении на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажение и пропадание данных, частые сообщения об ошибках и т.п.), пользователь должен поставить в известность сотрудника НТО ИТИБ и провести полную антивирусную проверку своей рабочей станции.

6.3. В случае обнаружения вируса, пользователь должен:

- прекратить работу (если завершение работы штатными средствами невозможно - отключить рабочую станцию от электрической сети);
- немедленно поставить в известность сотрудника НТО ИТИБ;
- совместно с сотрудником НТО ИТИБ провести лечение или уничтожение зараженных файлов.

7. РЕЗЕРВНОЕ КОПИРОВАНИЕ

7.1. Пользователю рекомендуется регулярно самостоятельно выполнять резервное копирование своих файлов на внешний носитель (usb-накопитель, жесткий или оптический диск и т.п.), либо на сетевой ресурс (облачное хранилище Института и т.п.).

7.2. Перед резервным копированием файлов необходимо завершить работу всех программ и закрыть все редактируемые документы.

7.3. Резервные копии данных в облачном хранилище Института должны храниться в архивированном виде (с целью экономии места).

7.4. Категорически **ЗАПРЕЩАЕТСЯ** хранить резервные копии вместе с исходными данными на одном физическом носителе (usb-накопителе, жёстком диске).

7.5. Пользователь несет персональную ответственность за целостность и сохранность рабочих файлов и документов на своей рабочей станции.

8. РАБОТА В ИНФОРМАЦИОННЫХ СИСТЕМАХ, В СЕТИ ИНТЕРНЕТ, С ЭЛЕКТРОННОЙ ПОЧТОЙ

8.1. Общие положения

8.1.1. Доступ к информационным системам, электронной почте Института и сети Интернет предоставляется пользователю Института в случае, если это не противоречит требованиям по информационной безопасности, указанным в политике информационной безопасности, данной Инструкции и иных нормативных документах Института.

8.1.2. Основанием для подключения рабочей станции пользователя к информационным системам, электронной почте, сети Интернет является заявка руководителю НТО ИТИБ от пользователя с указанием нужных сервисов для подключения.

8.1.3. После получения заявки сотрудник НТО ИТИБ организует подключение рабочей станции пользователя к указанным информационным ресурсам.

8.1.4. Сотрудники НТО ИТИБ осуществляют контроль над использованием в Институте информационных систем, электронной почты и сети Интернет.

8.1.5. Рабочая станция пользователя может быть отключена от информационных ресурсов Института, электронной почты и сети Интернет на основании:

- нарушения пользователем данной Инструкции и иных нормативных актов Института в области информационной безопасности;
- увольнения пользователя либо смены его обязанностей;
- обнаружения попыток несанкционированного доступа, компьютерных атак, а также расследования компьютерного инцидента;
- проведения технических работ.

8.2. Правила работы в сети Интернет

8.2.1. Использование сети Интернет в Институте осуществляется исключительно для выполнения должностных обязанностей.

8.2.2. Информация о ресурсах сети Интернет, посещаемых пользователями, протоколируется и может быть предоставлена руководству для анализа и принятия мер.

8.2.3. При использовании сети Интернет **ЗАПРЕЩАЕТСЯ:**

- предоставлять третьим лицам доступ в сеть Интернет со своей рабочей станции, в том числе программно-техническими способами;
- получать на рабочих станциях доступ к сети Интернет любым способом, кроме предоставленного Институтом (несанкционированно установленные GPRS-модемы, Wi-Fi-устройства и прочее), если это не согласовано с НТО ИТИБ. Основанием для использования данных устройств является заявление пользователя на имя руководителя НТО ИТИБ с указанием целей использования устройств и срока, в течение которого данные устройства будут использоваться. Заявление должно быть одобрено руководителем НТО ИТИБ. То же самое относится и к получению доступа к сети Интернет посредством технологии виртуальных частных сетей (VPN).

• открывать подозрительные ресурсы, переходить по подозрительным ссылкам, при открытии ресурса нужно убедиться в том, что он использует защищённое соединение (https://...)

8.3. Правила работы с электронной почтой

8.3.1. Корпоративная электронная почта Института предназначена исключительно для выполнения должностных обязанностей.

8.3.2. При работе с электронной почтой Института **ЗАПРЕЩАЕТСЯ:**

• рассылать почтовые сообщения одновременно на большое количество адресов, за исключением служебных объявлений;

• отправлять сообщения неэтичного или незаконного содержания;

• использовать рабочий адрес электронной почты для подписки на неслужебные почтовые рассылки (коммерческие, развлекательные и т.п.), а также для регистрации на сторонних сайтах (форумы, клубы и т.п.);

• отправлять и открывать при получении исполняемые или системные файлы (в частности, с расширениями bas, bat, bin, cab, cat, cmd, com, cpl, csh, dat, dll, dpl, drv, exe, inf, ins, inx, ipa, isu, jar, job, js, jse, ksh, lib, lnk, mdz, msc, msi, msp, mst, msu, nls, olb, osx, out, paf, pif, prg, pwz, reg, rgs, rom, run, scr, sct, sh, shb, shs, sys, tlb, vb, vbe, vbs, vbscript, vxd, workflow, ws, wsf, wsh), в том числе в составе архивных файлов;

• открывать вложенные файлы и ссылки, присланные в письмах от неизвестных отправителей, либо без предварительного запроса. При малейшем подозрении на то, что письмо может быть вирусным или мошенническим, необходимо писать или звонить в НТО ИТИБ.

9. ОТВЕТСТВЕННОСТЬ

Пользователь несет персональную (должностную, материальную, административную, уголовную) ответственность за свои действия или бездействие, которые повлекут за собой разглашение или утрату конфиденциальных (служебных, коммерческих, персональных и иных) данных, а также нарушение функционирования информационных систем, информационно-телекоммуникационной сети Института или ее отдельных компонентов, несанкционированный доступ к информации, нарушение требований настоящей Инструкции и других внутренних документов Института, регламентирующих правила работы в информационных системах, в соответствии с нормативными актами Института и законодательством Российской Федерации.