Приложение № 1
к приказу ГИН СО РАН
от «27» декабря 2018 № 68

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
Федерального государственного бюджетного учреждения науки Геологического института Сибирского отделения Российской академии наук (ГИН СО РАН)

Политика информационной безопасности Федерального государственного бюджетного учреждения науки Геологического института Сибирского отделения Российской академии наук (ГИН СО РАН) разработана в соответствии с: п. 2, 4, 6 ч. 1 и ч. 2 ст. 18.1 Федерального закона от 27.07.2006 N 152-ФЗ (ред. от 21.07.2014) "О персональных данных" (с изм. и доп., вступ. в силу с 01.09.2015); ст. 2 Перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных", и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами, утвержденного постановлением Правительства Российской Федерации от 21.03.2012 N 211 (ред. от 06.09.2014); п. 2.12, 4.1 - 4.3 ГОСТ Р ИСО/МЭК 13335-1-2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий; п. 3.1.48, А.6.3 ГОСТ Р ИСО/МЭК 15408-1-2012 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий.

Политика информационной безопасности ГИН СО РАН определяет общую совокупность документированных правил, процедур, практических

приемов и руководящих принципов в области безопасности информации, которыми руководствуется ГИН СО РАН в своей деятельности.

Целью Политики информационной безопасности (далее – Политики) является определение основных правил обеспечения безопасности объектов защиты ГИН СО РАН от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных, а также минимизации ущерба от возможной реализации угроз безопасности защищаемой информации. Структура Политики разработана в соответствии с Примерным перечнем вопросов, входящих в состав политики безопасности информационных технологий организации.

I. Область применения

Настоящая Политика определяет общие правила, процедуры, практические приемы и руководящие принципы в области безопасности информации, которыми руководствуется ГИН СО РАН в своей деятельности и которые применяются для регламентирования единых подходов в ГИН СО РАН к построению системы защиты информации информационных систем (далее – СЗИИС).

В Политике определены объекты защиты, общий замысел защиты информации ГИН СО РАН, принципы построения системы защиты информационных систем, требования к пользователям информационных систем, степень ответственности персонала, структура и необходимый уровень защищенности, статус и должностные обязанности лиц, ответственных за обеспечение безопасности информации, обрабатываемой в информационных системах ГИН СО РАН.

Требования Политики обязательны для всех работников ГИН СО РАН, представителей контрольно-надзорных органов, допущенных к защищаемой информации на законных основаниях, а также индивидуальных лиц и работников иных организаций, допущенных к защищаемой информации для

проведения работ по государственным контрактам или иным гражданско-правовым договорам.

II. Термины, обозначения и сокращения

В настоящей Политике используются следующие термины и обозначения:

Автоматизированная обработка персональных данных - обработка персональных данных с помощью средств вычислительной техники.

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

Администратор безопасности информации - лицо, отвечающее за защиту информационных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации объекта информатизации.

Анализ уязвимостей - мероприятия по выявлению, идентификации и оценке уязвимостей информационной системы в интересах определения возможности реализации угроз безопасности информации и способов предотвращения ущерба.

Аттестация объектов информатизации - комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации.

Аутентификация - проверка принадлежности субъекту доступа предъявленного им идентификатора (подтверждение подлинности субъекта доступа в информационной системе).

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

Виртуализация - технология преобразования формата или параметров программных, или сетевых запросов к компьютерным ресурсам с целью обеспечения независимости процессов обработки информации от программной или аппаратной платформы информационной системы.

Вредоносная программа - программа, используемая для несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной информационной системы.

Доступность (санкционированная доступность) информации - состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Замысел защиты информации - основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации.

Информационная система персональных данных (ИСПДн) - совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств.

Информационные системы ГИН СО РАН - информационные системы, включая информационные системы персональных данных, представляющие собой совокупность информации, содержащейся в базах данных, и обеспечивающих ее обработку информационных технологий и технических средств.

Инцидент - непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Компьютерный вирус - программа, способная создавать свои копии (необязательно совпадающие с оригиналом) и внедрять их в файлы, системные области компьютера, компьютерных сетей, а также осуществлять иные деструктивные действия. При этом копии сохраняют способность дальнейшего распространения. Компьютерный вирус относится к вредоносным программам.

Контролируемая зона - это пространство, в котором исключено неконтролируемое пребывание работников и посетителей оператора и посторонних транспортных, технических и иных материальных средств.

Криптографические средства защиты информации - средства шифрования - аппаратные, программные и аппаратно-программные средства, системы и комплексы, реализующие алгоритмы криптографического преобразования информации и предназначенные для защиты информации при передаче по каналам связи и (или) для защиты информации от несанкционированного доступа при ее обработке и хранении.

Машинные носители информации - физическое устройство (дискета, e-Token, смарт-карта и т.д.), предназначенное для хранения информации в электронной форме.

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

Модель угроз - физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

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

Обработка информации - совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи хранения, регистрации,

уничтожения, преобразования, отображения, осуществляемых над информацией.

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

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

Объект защиты информации - информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

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, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров.

Организационные меры защиты информации - под организационными мерами (оргмерами) понимаются организационные мероприятия по обеспечению физической защиты информации, предусматривающие установление режимных, временных, территориальных, пространственных ограничений на условия использования и распорядок работы объекта защиты.

Оператор информационной системы - гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы,

Оператор персональных данных (оператор ПДн) - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными.

Ответственный за организацию обработки персональных данных - должностное лицо оператора ПДн (ГИН СО РАН), осуществляющее:

- внутренний контроль за соблюдением работниками законодательства Российской Федерации о персональных данных, в том числе требований к защите персональных данных;
- доведение до сведения работников ГИН СО РАН положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;
- организацию, прием и обработку обращений и запросов субъектов персональных данных или их представителей и (или) осуществляющее контроль за приемом и обработкой таких обращений и запросов;
- контроль организации допуска работников ГИН СО РАН к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных).

Политика безопасности (информации в организации) - совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

Программная среда - совокупность программного обеспечения, используемого в информационной системе для решения одной или нескольких задач.

Регуляторы - Федеральная служба по техническому и экспортному контролю (ФСТЭК России), Федеральная служба безопасности (ФСБ России), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

Роль - предопределенная совокупность правил, устанавливающих допустимое взаимодействие между пользователем и информационной системой.

Система защиты информации информационных систем (СЗИИС) - система защиты информации информационных систем включает в себя организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности защищаемой информации и информационных технологий, используемых в информационных системах.

Технические меры защиты информации - под техническими мерами защиты информации в узком смысле слова понимается защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Угрозы безопасности персональных данных - совокупность условий и факторов, создающих опасность несанкционированного, в том числе случайного, доступа к персональным данным, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий при их обработке в информационной системе персональных данных.

Управление доступом - ограничение и контроль доступа субъектов доступа к объектам доступа в информационной системе в соответствии с установленными правилами разграничения доступа.

Уязвимость информационной системы - недостаток (слабость) информационной системы, который (которая) создает потенциальные или реально существующие условия для реализации или проявления угроз безопасности информации.

Целостность информации - устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

Цель защиты информации - заранее намеченный результат защиты информации.

В настоящем Положении используются следующие сокращения:

АС - автоматизированная система;

ИС - информационная система;

ИСПДн - информационная система персональных данных;

КЗ - контролируемая зона;

КСЗИ - криптографическое средство защиты информации;

МНИ - машинные носители информации;

МЭ - межсетевой экран;

НСД - несанкционированный доступ;

оргмеры - организационные меры защиты персональных данных;

ПДн - персональные данные;

СЗИ - средства защиты информации;

СЗИИС - система защиты информации информационных систем;

СЭД - система электронного документооборота

III. Объекты и общий замысел защиты информации ГИН СО РАН

Объектами защиты ГИН СО РАН являются:

- информационные ресурсы, содержащие конфиденциальную информацию, а также открытая (общедоступная) информация, необходимая для работы ГИН СО РАН, независимо от формы и вида ее представления;

- процессы обработки информации в информационных системах ГИН СО РАН, информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;

- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены элементы информационной среды.

Общий замысел защиты информации исходит из того, что:

- безопасность защищаемой информации достигается путем исключения несанкционированного, в том числе случайного, доступа к защищаемой конфиденциальной информации (включая и персональные данные), результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение защищаемой информации, а также иных несанкционированных действий;

- выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и осуществления конкретных мероприятий по обеспечению безопасности конфиденциальной информации (включая и персональные данные) в ГИН СО РАН;

- информация и связанные с ней ресурсы должны быть доступны для авторизованных пользователей.

Защита информации исполняется в соответствии с: п. 12, 20, 20.10 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 №

17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный N 28608), а также раздел X приложения № 2 к указанным Требованиям; п. 1.9, 6.3.9 Специальных требований и рекомендаций по технической защите конфиденциальной информации (СТР-К), утвержденных приказом Гостехкомиссии России от 30.08.2002 № 282. и ГИН СО РАН обязан:

- осуществлять своевременное обнаружение и реагирование на угрозы безопасности персональных данных;

- осуществлять предотвращение преднамеренных или случайных, частичных или полных несанкционированных модификаций или уничтожения данных.

Основополагающим принципом построения системы защиты информации информационных систем ГИН СО РАН является следующее положение: в соответствии с положениями нормативных правовых актов Регуляторов и внутренних распорядительных актов в ГИН СО РАН применяются требования для защиты информации, содержащейся в государственных информационных системах.

IV. Цели, задачи и принципы обеспечения информационной безопасности в ГИН СО РАН

Цели обеспечения информационной безопасности в ГИН СО РАН

В соответствии с: ст. 9, ч. 1 и ч. 5 ст. 16 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 31.12.2014) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.09.2015); п. 12 Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11.02.2013 № 17 (зарегистрировано в Министерстве юстиции Российской Федерации 31.05.2013, регистрационный N 28608) установлены следующие цели обеспечения защиты информации ограниченного доступа в ГИН СО РАН:

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

- соблюдение конфиденциальности информации ограниченного доступа;

- реализация права на доступ к информации.

Задачи обеспечения информационной безопасности в ГИН СО РАН

Для достижения целей защиты информации в ГИН СО РАН создается система информационной безопасности, включающая в себя систему защиты информации информационных систем и внутренние организационно-распорядительные акты, регламентирующие обращение защищаемой информации как на электронных, так и на бумажных носителях.

Система защиты информации информационных систем ГИН СО РАН призвана решать задачи:

- идентификации и аутентификации субъектов доступа и объектов доступа;
- управления доступом субъектов доступа к объектам доступа;
- ограничения программной среды;
- защиты машинных носителей информации;
- регистрации событий безопасности;
- антивирусной защиты;
- обнаружения (предотвращения) вторжений;
- контроля (анализа) защищенности информации;
- целостности информационной системы и информации;
- доступности информации;
- защиты технических средств;
- защиты среды виртуализации;
- защиты информационной системы, ее средств, систем связи и передачи данных.

V. Организация и инфраструктура информационной безопасности в ГИН СО РАН

Организация информационной безопасности в ГИН СО РАН заключается в:

- определении лиц, ответственных за организацию и поддержание информационной безопасности в ГИН СО РАН;

- регламентации оборота конфиденциальной информации на бумажных и электронных носителях;

- построении, аттестации и вводе в эксплуатацию системы защиты информационных систем;

- обучении пользователей по вопросам информационной безопасности.

Лица, ответственные за организацию и поддержание информационной безопасности в ГИН СО РАН:

- председатель как первый руководитель ГИН СО РАН несет персональную ответственность за регламентацию порядка безопасной обработки конфиденциальной информации и обеспечение требований по технической защите конфиденциальной информации.

- администратор безопасности информации, несущий ответственность за защиту информационных систем от несанкционированного доступа к информации, за эксплуатацию средств и мер защиты информации, обучение назначенных лиц специфике работ по защите информации на стадии эксплуатации информационных систем.

- администратор безопасности и системный администратор, несущий ответственность за поддержание уровня защищенности информационных систем ГИН СО РАН.

- лицо, ответственное за организацию обработки персональных данных, несет ответственность за:

- осуществление внутреннего контроля за соблюдением работниками законодательства Российской Федерации о защите персональных данных, в том числе требований к защите персональных данных;

- доведение до сведения работников ГИН СО РАН положения законодательства Российской Федерации о персональных данных, локальных актов по вопросам обработки персональных данных, требований к защите персональных данных;

- организацию приема и обработки обращений и запросов субъектов персональных данных или их представителей и (или) осуществлении контроля за приемом и обработкой таких обращений и запросов;

- осуществление контроля организации допуска работников ГИН СО РАН к информации, в отношении которой установлено требование об обеспечении ее конфиденциальности.

Система защиты информации информационных систем в ГИН СО РАН должна строиться на основании применения правовых, организационных и технических мер по обеспечению безопасности защищаемой информации.

В организационно-распорядительных документах определяется необходимый уровень защищенности информации информационных систем ГИН СО РАН. На основании анализа актуальных угроз безопасности информации, необходимо сделать заключение о необходимости использования технических средств и организационных мероприятий для обеспечения безопасности защищаемой информации. Выбранные необходимые технические мероприятия отражены в Плане мероприятий защиты информации информационных систем.

В зависимости от уровня защищенности информационных систем, актуальных угроз и предъявляемых требований к защите информации система защиты включает следующие технические средства:

- антивирусные средства для рабочих станций пользователей и серверов;

- средства межсетевого экранирования;

- система защиты информации от НСД;

- средства криптографической защиты информации при передаче защищаемой информации по каналам связи.

Обучение пользователей по вопросам информационной безопасности

Перед допуском к самостоятельной работе с информацией ограниченного доступа пользователи должны быть соответствующим образом проинструктированы администратором безопасности информации (или уполномоченным лицом, на которого возложены обязанности по защите информации) или иным образом обучены правилам обращения с конфиденциальной информацией и средствами защиты информации.

Инфраструктура информационной безопасности в ГИН СО РАН заключается в:

определении ролей и обязанностей должностных лиц по обеспечению информационной безопасности;

регулярной проверке согласованности мер защиты информации;

обработке инцидентов, связанных с нарушением безопасности.

Определение ролей и обязанностей должностных лиц по обеспечению информационной безопасности

Администратор информационной системы:

Администратор информационной системы - должностное лицо ГИН СО РАН или уполномоченное лицо (работник уполномоченного лица), ответственное за настройку, внедрение и сопровождение информационных систем. Администратор информационной системы обеспечивает функционирование подсистемы управления доступом ИС и уполномочен осуществлять предоставление и разграничение доступа конечного пользователя к элементам, хранящим защищаемую информацию.

Администратор информационной системы обладает следующим уровнем доступа и знаний:

- обладает полной информацией о системном и прикладном программном обеспечении ИС;

- обладает полной информацией о технических средствах и конфигурации ИС;

- имеет доступ ко всем техническим средствам обработки информации и данным ИС;

- обладает правами конфигурирования и административной настройки технических средств ИС.

Администратор безопасности информации:

Администратор безопасности информации - должностное лицо ГИН СО РАН или уполномоченное лицо (работник уполномоченного лица), ответственное за функционирование СЗИИС, включая обслуживание и настройку административной, серверной и клиентской компонент.

Администратор безопасности информации обладает следующим уровнем доступа и знаний:

- обладает правами администратора ИС;
- обладает полной информацией об ИС;
- имеет доступ к средствам защиты информации и протоколирования, а также к части ключевых элементов ИС;
- имеет права доступа к конфигурированию технических средств сети, за исключением контрольных (инспекционных).

Администратор безопасности информации уполномочен:

- реализовывать политики безопасности в части настройки СКЗИ, межсетевых экранов и систем обнаружения атак, в соответствии с которыми пользователь получает возможность работать с элементами ИС;

- осуществлять аудит средств защиты;

- устанавливать доверительные отношения своей защищенной сети с сетями других органов власти и организаций.

Пользователь - должностное лицо ГИН СО РАН или иного государственного (муниципального) органа (организации), допущенное в

установленном порядке к работе с защищаемой информацией, полномочия которого регламентированы внутренними организационно-распорядительными актами ГИН СО РАН. Обработка защищаемой информации включает: возможность просмотра информации, ручной ввод информации в информационную систему, формирование справок и отчетов по информации, полученной из ИС. Пользователь не имеет полномочий для управления подсистемами обработки данных и СЗИИС.

Пользователь обладает следующим уровнем доступа и знаний:

- обладает всеми необходимыми атрибутами (например, паролем), обеспечивающими доступ к некоторому подмножеству защищаемой информации;

- располагает конфиденциальными данными, к которым имеет доступ. Конкретизация ролей производится в должностных обязанностях лиц, допущенных к работе в ИС.

Регулярная проверка согласованности мер защиты информации

В ГИН СО РАН должны проводиться следующие мероприятия по проверке согласованности мер защиты информации:

- поддержание в актуальном состоянии организационных мер защиты информации;

- контроль неизменности защищаемой инфраструктуры;

- контроль работоспособности средств защиты информации;

- выявление и анализ уязвимостей ИС.

Обработка инцидентов, связанных с нарушением безопасности информации

В ГИН СО РАН должны проводиться следующие мероприятия по обработке инцидентов, связанных с нарушением безопасности информации:

- определение лиц, ответственных за выявление инцидентов и реагирование на них;

- обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств,

программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- своевременное информирование лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе пользователями и администраторами;

- анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

- планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

- планирование и принятие мер по предотвращению повторного возникновения инцидентов.

VI. Безопасность аппаратно-программного обеспечения в ГИН СО РАН

Безопасность аппаратно-программного обеспечения в ГИН СО РАН должна достигаться проведением следующих мероприятий:

- идентификацией и аутентификацией субъектов доступа;

- управлением доступом субъектов доступа к объектам доступа;

- мониторингом (просмотром, анализом) результатов регистрации событий безопасности и реагирование на них;

- уничтожением (стиранием) данных и остаточной информации с машинных носителей информации и (или) уничтожением машинных носителей информации;

- антивирусной защитой;

- обеспечением безопасности персональных компьютеров;

- обеспечением безопасности среды виртуализации;

- регламентацией и контролем использования в информационной системе мобильных технических средств;

- установкой (инсталляцией) только разрешенного к использованию программного обеспечения и (или) его компонентов.

Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них

Мониторинг результатов регистрации событий безопасности должен проводиться в форме анализа системных журналов и журналов СЗИ, проводимого администратором безопасности информации с целью своевременного выявления факта попыток несанкционированного доступа к информационным ресурсам в информационные системы ГИН СО РАН.

Анализ журналов должен производиться ежедневно. При анализе журналов СЗИ НСД проверяются:

- журналы контроля целостности программных частей СЗИ;

- журналы контроля целостности программного обеспечения ИС;

- журналы доступа пользователей и процессов к защищаемым объектам;

- журналы создания новых пользователей в СЗИ и изменения полномочий пользователей.

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации и (или) уничтожение машинных носителей информации

Уничтожение (стирание) данных и остаточной информации с машинных носителей информации в ГИН СО РАН должно производиться при необходимости передачи машинного носителя информации другому пользователю информационной системы или в сторонние организации для ремонта, технического обслуживания или дальнейшего уничтожения.

При выводе из эксплуатации машинных носителей информации, на которых осуществлялись хранение и обработка информации, в

установленном порядке должно осуществляться физическое уничтожение этих машинных носителей информации.

Антивирусная защита в информационных системах ГИН СО РАН

Безопасность аппаратно-программного обеспечения в ГИН СО РАН от разрушающего воздействия компьютерных вирусов достигается также проведением мероприятий по антивирусной защите, основанных на следующих принципах:

- контроль состояния антивирусной защиты ИС ГИН СО РАН возлагается на администратора безопасности информации;

- к использованию в ИС допускаются только сертифицированные антивирусные средства, централизованно закупленные у разработчиков (или официальных поставщиков) указанных средств

- ежедневно в начале работы при загрузке компьютеров в автоматическом режиме обязан проводиться автоматический контроль всех дисков и файлов;

- должно обеспечиваться автоматическое централизованное обновление вирусных сигнатур и антивирусного ПО на всех ПЭВМ, работающих в ИС;

- обязательному автоматическому антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), информация на съемных (несъемных) носителях (магнитных дисках, CD-ROM, флэш и т.п.);

- файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль. Периодические проверки электронных архивов должны проводиться не реже одного раза в месяц;

- устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов.

Обеспечение безопасности персональных компьютеров ГИН СО РАН

Безопасность персональных компьютеров в ГИН СО РАН должна достигаться осуществлением мер физического и логического контроля доступа.

Меры физического контроля доступа к средствам вычислительной техники (физическая защита) регламентируются нормативными правовыми актами Регуляторов и внутренними организационно-распорядительными актами.

Политика в отношении логического доступа к компьютерам заключается в:

- установлении правил разграничения доступа и контроля соблюдения этих правил;

- контроле доступа пользователей к СВТ информационной системы с целью предотвращения неавторизованного доступа к информационным системам (контроле регистрации пользователей, управлении привилегиями доступа, контроле в отношении паролей пользователей, пересмотре прав доступа пользователей и др.).

Обеспечение безопасности среды виртуализации

Для обеспечения безопасности виртуальной среды должны применяться меры защиты, аналогичные применяемым в физической среде, но с учетом специфических особенностей виртуальной среды, а именно:

- идентификация и аутентификация субъектов доступа как внутри виртуальной среды, так и при доступе к средствам управления виртуальной инфраструктурой;

- управление доступом субъектов доступа к объектам доступа внутри виртуальной среды и при доступе к средствам управления этой средой;

- управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры;

- регистрация событий безопасности в виртуальной инфраструктуре;

- управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных;

- контроль целостности виртуальной инфраструктуры и ее конфигураций;

- резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры;

- реализация и управление антивирусной защитой в виртуальной инфраструктуре;

-разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

VII. Телекоммуникационная безопасность ГИН СО РАН

С целью защиты как внутренних, так и внешних сетевых сервисов в ГИН СО РАН должен осуществляться контроль сетевого доступа, для обеспечения которого при необходимости определяются:

политика в отношении использования сетевых служб;

предопределенный маршрут;

аутентификация пользователей в случае внешних соединений;

принципы разделения в сетях;

контроль сетевых соединений;

управление маршрутизацией сети;

безопасность использования сетевых служб;

политика в отношении электронной почты.

Политика в отношении использовании сетевых служб

В ГИН СО РАН установлен разрешительный режим доступа к сетевым службам.

В связи с тем, что несанкционированные подключения к сетевым службам могут нарушать информационную безопасность ГИН СО РАН,

пользователям должен обеспечиваться непосредственный доступ только к тем сервисам, в которых они были авторизованы.

В целях контроля сетевого доступа должны определяться:

- сети и сетевые услуги, к которым разрешен доступ;
- процедуры авторизации для определения кому, к каким сетям и сетевым сервисам разрешен доступ;
- мероприятия и процедуры по защите от несанкционированного подключения к сетевым сервисам.

Аутентификация узлов в случае внешних соединений

Аутентификация узлов в случае внешних соединений в ГИН СО РАН должна достигаться средствами криптографии.

Принцип разделения в сетях

В ГИН СО РАН по управлению информационной безопасностью в пределах сети должны разделяться группы информационных сервисов, пользователей и информационные системы.

Критерии для разделения сетей на домены формируются на основе анализа политики контроля доступа, а также учитывая влияние этого разделения на производительность в результате включения подходящей технологии маршрутизации сетей или шлюзов.

Контроль сетевых соединений

В ГИН СО РАН для контроля сетевого доступа должны применяться мероприятия по управлению информационной безопасностью, чтобы ограничивать возможности пользователей по подсоединению. Такие мероприятия могут быть реализованы посредством сетевых шлюзов, которые фильтруют трафик с помощью определенных таблиц или правил. Применяемые ограничения должны основываться на политике и требованиях доступа к бизнес-приложениям, а также соответствующим образом поддерживаться и обновляться.

Ограничения должны применяться к следующим бизнес-приложениям:

- электронная почта;

- передача файлов в одном направлении;
- передача файла в обоих направлениях;
- интерактивный доступ;
- доступ к сети, ограниченный определенным временем суток или датой.

Политика в отношении электронной почты

В ГИН СО РАН для обеспечения информационной безопасности должны быть регламентированы правила использования электронной почты, предусматривающие следующие аспекты:

- вероятность атаки на электронную почту (вирусы, перехват);
- защиту вложений в сообщения электронной почты;
- данные, при передаче которых не следует пользоваться электронной почтой;
- исключение возможности компрометации ГИН СО РАН со стороны сотрудников, например, путем рассылки дискредитирующих и оскорбительных сообщений, использование корпоративной электронной почты с целью неавторизованных покупок;
- использование криптографических методов для защиты конфиденциальности и целостности электронных сообщений;
- хранение сообщений, которые в этом случае могли бы быть использованы в случае судебных разбирательств;
- дополнительные меры контроля обмена сообщениями, которые не могут быть аутентифицированы.

VIII. Физическая безопасность в ГИН СО РАН

Физическая безопасность в ГИН СО РАН должна достигаться проведением мероприятий, касающихся как внешних, так и внутренних аспектов.

Физическая безопасность от внешних угроз должна достигаться:

- установлением контролируемой зоны;

- контролем доступа посторонних лиц в помещения контролируемой зоны в рабочее и нерабочее время.

Физическая безопасность от внутренних угроз должна достигаться:

- прочностью строительных конструкций здания;

- противопожарной защитой и пожарной сигнализацией;

- регламентацией действий персонала при возгорании, предотвращении и (или) минимизации ущерба при затоплении водой/жидкостью, отключении электроэнергии;

- защитой коммуникаций и систем обеспечения энергоносителями в зданиях;

- размещением оборудования, исключающим несанкционированный доступ к нему и несанкционированный доступ к видовой информации.

IX. Безопасность персонала ГИН СО РАН

Вопросы безопасности, связанные с персоналом, заключаются в:

- учете вопросов безопасности при найме персонала;

- включении вопросов информационной безопасности в должностные обязанности;

- соглашении о конфиденциальности;

- условиях трудового договора;

- обучении пользователей;

- реагировании на инциденты нарушения информационной безопасности и сбои.

Включение вопросов информационной безопасности в должностные обязанности

Функции (роли) и ответственность в области информационной безопасности следует документировать. В должностные обязанности работников ГИН СО РАН должны включаться как общие обязанности по внедрению или соблюдению политики безопасности, так и специфические

особенности по защите определенных активов или действий, касающихся безопасности.

Соглашение о конфиденциальности

В ГИН СО РАН регламентирован порядок доступа работников ГИН СО РАН и сотрудников иных органов и организаций к конфиденциальной информации. Соглашение о конфиденциальности заключается в форме Обязательства работника о неразглашении конфиденциальной информации ГИН СО РАН и Соглашения о неразглашении конфиденциальной информации ГИН СО РАН, заключаемого с сотрудниками иных органов и организаций, допускаемых к конфиденциальной информации на основании государственных контрактов или гражданско-правовых договоров.

В государственные контракты и гражданско-правовые договоры, заключаемые ГИН СО РАН с подрядчиками, которым для выполнения условий контракта (договора) необходим доступ к служебной информации, в соответствии с нормами действующего законодательства включаются положения о соблюдении конфиденциальности.

Условия трудового договора

В ГИН СО РАН в соответствии с действующим законодательством устанавливаются условия трудового договора, определяющего ответственность работника в отношении информационной безопасности. Указанная ответственность сохраняется и в течение 36 месяцев после увольнения со службы. До работника доводятся меры ответственности, которые будут применимы в случае нарушения требований безопасности.

Информирование о проблемах безопасности

В обязанностях пользователей информационных сервисов предусматривается, что они должны:

обращать внимание и сообщать о любых замеченных или предполагаемых недостатках и угрозах в области безопасности в системах или сервисах;

немедленно сообщать об этих причинах для принятия решений своему руководству или непосредственно поставщику услуг.

Требования информационной безопасности предусматривают, что пользователи не должны ни при каких обстоятельствах самостоятельно искать подтверждения подозреваемому недостатку в системе безопасности.

Для информирования о сбоях программного обеспечения в ГИН СО РАН регламентированы соответствующие процедуры, при которых должны предусматриваться следующие действия:

симптомы проблемы и любые сообщения, появляющиеся на экране, должны фиксироваться;

по возможности, компьютер необходимо изолировать и пользование им прекратить;

о факте сбоя программного обеспечения немедленно должен извещаться администратор безопасности информации.

Пользователи не должны пытаться самостоятельно удалить подозрительное программное обеспечение, если они не уполномочены на это. Ликвидировать последствия сбоев должен соответственно обученный персонал.

Процесс установления дисциплинарной ответственности

По каждому выявленному факту нарушения информационной безопасности в ГИН СО РАН регламентировано проведение служебной проверки и привлечение виновных к ответственности.

X. Безопасность документов и носителей информации в ГИН СО РАН

В ГИН СО РАН в целях информационной безопасности регламентирован полный цикл обращения конфиденциальных документов, в том числе и на электронных носителях (создание или получение, регистрация, пересылка, исполнение, хранение, уничтожение).

Контроль выполнения правил документооборота (в том числе и конфиденциального) в ГИН СО РАН должен осуществляться ответственным на то лицом.

Контроль за оборотом (учетом, выдачей, использованием, передачей, хранением и уничтожением) машинных носителей информации должен осуществляться администратором безопасности информации.

XI. Политика аутсорсинга в ГИН СО РАН

В соответствии с требованиями действующего законодательства ГИН СО РАН вправе поручить на договорной основе уполномоченным лицам исполнять следующие функции обеспечения безопасности:

физическая защита (охрана помещений, пропускной режим, обслуживание охранно-пожарной сигнализации);

администрирование информационных систем;

администрирование информационной безопасности и др.

Лицо, обрабатывающее информацию, являющуюся государственным информационным ресурсом, по поручению ГИН СО РАН и (или) предоставляющее ГИН СО РАН вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся государственным информационным ресурсом, в соответствии с требованиями по защите информации и настоящей Политикой.

XII. Ответственность и полномочия

Ответственность персонала

За нарушение требований настоящей Политики должностные лица ГИН СО РАН несут ответственность в соответствии с действующим законодательством.

Должностные лица ГИН СО РАН, вносящие изменения в конфигурацию информационных систем и СЗИИС, несут ответственность за соответствие своих действий процедурам, регламентированным настоящей Политикой.

Полномочия персонала

Работники ГИН СО РАН имеют право выходить с предложениями к руководству ГИН СО РАН по вопросам защиты конфиденциальной информации. Изменения в настоящую Политику вносятся приказом ГИН СО РАН после обязательного согласования вносимых изменений с главным специалистом сектора по информационной безопасности, отвечающим за соответствие вносимых изменений требованиям законодательства и нормативно-правовых актов Регуляторов.

Приложение № 2
к приказу ГИН СО РАН
от «__» _____2019 № 269-____

ПЛАН МЕРОПРИЯТИЙ
ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ
Федерального государственного бюджетного учреждения науки Геологического института Сибирского отделения Российской академии наук (ГИН СО РАН)

N п/п	Мероприятия	Сроки	Исполнитель	Примечания
Организационные мероприятия				
1	Первичная внутренняя проверка	разовое, срок до 01.01.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	
2	Определение обрабатываемых ПДн и объектов защиты	разовое, срок до 01.01.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	
3	Определение круга лиц, участвующих в обработке защищаемой информации	разовое, срок до 01.01.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	
4	Определение ответственности лиц, участвующих в обработке конфиденциальной информации	разовое, срок до 01.01.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	
5	Определение прав разграничения доступа пользователей ИС, необходимых для выполнения должностных обязанностей	разовое, срок до 01.01.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	
6	Разработка Положения об администраторе безопасности информации	разовое, срок до 01.01.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	
7	Введение режима защиты конфиденциальной информации	разовое, срок до 01.01.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	

8	Первичный анализ актуальности угроз безопасности конфиденциальной информации, обрабатываемой в ИС	разовое, срок до 01.01.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	
9	Организация режима и контроля доступа (охраны) в помещения, в которых установлены аппаратные средства ИС и СКЗИ (средства криптографической защиты информации)	разовое, срок до 01.01.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	
10	Внесение изменений в должностные инструкции о порядке обработки конфиденциальной информации и обеспечении введенного режима защиты, согласно изменениях в нормативных актах	по мере необходимости	Зангеева С.А. Бальжинимаева Ю.Г.	
11	Корректировка организационно-распорядительной документации по защите конфиденциальной информации	по мере необходимости	Зангеева С.А. Бальжинимаева Ю.Г.	
12	Организация пропуска в контролируемую зону в рабочее и нерабочее время	разовое, срок до 01.02.2020	Зангеева С.А Бальжинимаева Ю.Г. Минеев А.В	
Технические (аппаратные и программные) мероприятия				
13	Анализ рынка, мероприятия по закупкам, внедрение подсистемы обнаружения вторжений и защиты от НСД (несанкционированного доступа)	не реже 1 раза в 3 года	Бальжинимаева Ю.Г. Минеев А.В.	
Аттестационные мероприятия				

14	Проведение аттестационных испытаний и получение аттестата соответствия СЗИИС требованиям законодательства	В случае необходимости	специализированная организация - лицензиат ФСТЭК	
Контролирующие мероприятия				
15	Контроль соответствия ИС требованиям по защите информации от НСД и эффективности функционирования СЗИ от НСД	не реже 1 раза в 3 года	специализированная организация - лицензиат ФСТЭК	
16	Инструментальный контроль эффективности системы защиты информации информационных систем	не реже 1 раза в 3 года	специализированная организация - лицензиат ФСТЭК	