

УТВЕРЖДЕНО

приказом Статкомитета СНГ

от « 03 » 02 2020 г. № 5

**Перечень документов
по защите информационных ресурсов ПАК ИАП в локальной вычислительной
сети Статкомитета СНГ**

№ п.п	Название документа
1.	Инструкция по организации парольной защиты автоматизированных рабочих мест пользователей в локальной вычислительной сети Статкомитета СНГ
2.	Инструкция по организации антивирусной защиты в локальной вычислительной сети Статкомитета СНГ
3.	Инструкция администратора базы данных локальной вычислительной сети Статкомитета СНГ
4.	Инструкция администратора локальной вычислительной сети Статкомитета СНГ
5.	Инструкция администратора информационной безопасности локальной вычислительной сети Статкомитета СНГ
6.	Инструкция пользователя персонального компьютера при работе в локально-вычислительной сети Статкомитета СНГ
7.	Инструкция по порядку резервирования, хранения и уничтожения массивов и носителей информации в Статкомитете СНГ
8.	Технология беспроводных коммуникаций в локальной вычислительной сети Статкомитета СНГ
9.	Порядок использования электронной почты в Статкомитете СНГ
10.	Порядок по контролю и анализу защищенности информационных ресурсов Статкомитета СНГ
11.	Рекомендации по физической защите объектов информатизации Статкомитета СНГ
12.	Положение о конфиденциальной информации Статкомитета СНГ

УТВЕРЖДЕНО
приказом Статкомитета СНГ
от « 03 » 02 2020 г. № 5

**ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ
АВТОМАТИЗИРОВАННЫХ РАБОЧИХ МЕСТ ПОЛЬЗОВАТЕЛЕЙ
В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ СТАТКОМИТЕТА СНГ**

1. ОБЩИЕ СВЕДЕНИЯ

Инструкция по организации парольной защиты регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) Информационно-телекоммуникационной системы (далее - Системы) Статкомитета СНГ, на автоматизированных рабочих местах, а также контроль за действиями пользователей и обслуживающего персонала Системы при работе с паролями.

Пользователь несёт персональную ответственность за сохранение в тайне своего пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам информационных отделов, записывать его, а также пересылать открытым текстом в электронных сообщениях.

В случае компрометации пароля (либо подозрения на компрометацию) пользователь обязан немедленно сообщить об этом администратору информационной безопасности и самостоятельно произвести смену основного пароля.

Плановая смена паролей пользователей должна проводиться регулярно, рекомендуется не реже одного раза в месяц.

Повседневный контроль за действиями пользователей при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на администраторов информационной безопасности.

2. ПОРЯДОК ПОЛУЧЕНИЯ ПАРОЛЯ ДОСТУПА К ЛВС

Для получения пароля доступа к локальной вычислительной сети (ЛВС) Статкомитета СНГ каждый сотрудник должен оформить заявку на имя руководителя ИТ-отдела, утвержденную руководителем структурного подразделения или ответственным должностным лицом, уполномоченным приказом председателя Статкомитета СНГ.

В заявке определяются необходимые ресурсы Системы и права доступа к ним.

На основании заявки сотрудник включается в группы пользователей и получает пароль доступа к ЛВС в соответствии с политикой безопасности, установленной для этих групп.

Обеспечение доступа к ЛВС Статкомитета СНГ выполняет администратор ЛВС.

Сотруднику предоставляется индивидуальная учетная запись пользователя и временный пароль. Бланк с учетными данными выдается сотруднику под подпись администратором ЛВС.

При создании учетной записи администратор ЛВС устанавливает опцию, требующую смены временного пароля при первом доступе к ЛВС, а также уведомляет владельца учетной записи о необходимости произвести смену пароля. Временный пароль не дает права доступа к ресурсам ЛВС, а служит для создания основного пароля пользователя, известного лишь лицу, создавшему пароль.

Первый вход в ЛВС сотрудник (пользователь) осуществляет с именем учетной записи и временным паролем, предоставленным администратором ЛВС. Пользователь производит замену временного пароля на основной и в дальнейшем доступ к ЛВС осуществляет с созданным им основным паролем. Количество символов в пароле должно быть не менее 8 (восемь).

При выборе пароля необходимо руководствоваться требованиями к паролям, изложенными в разделе 4 «Требования к паролям».

Для предоставления доступа другому пользователю к информации, хранящейся на рабочей станции и файловых серверах пользователя, отсутствующего на рабочем

месте в случае его болезни, командировки или отпуска руководитель структурного подразделения направляет служебную записку на имя руководителя ИТ-подразделения. В служебной записке должны быть указаны фамилия, имя и отчество сотрудника, которому разрешается доступ к информации отсутствующего пользователя, а также дата начала и срок действия доступа. Пользователю, которому разрешается доступ к информации отсутствующего пользователя, администратор ЛВС предоставляет имя учетной записи, временный пароль и устанавливает опцию, требующую смены пароля. Бланк с учетными данными выдается пользователю под подпись администратором ЛВС. По окончании срока действия доступа учетная запись отключается, а доступ к ресурсам ЛВС блокируется.

Для предотвращения подбора паролей администратор ЛВС обязан настроить механизм блокировки учётной записи. Разблокирование учётной записи пользователя осуществляется администратором ЛВС на основании служебной записки руководителя соответствующего структурного подразделения.

3. ПОРЯДОК ПОЛУЧЕНИЯ ПАРОЛЯ ДОСТУПА К БД

Для обработки в соответствии со своими служебными обязанностями информации, содержащейся в базах данных Системы, сотрудник оформляет заявку на обеспечение доступа к информационным ресурсам баз данных Системы.

Заявка оформляется сотрудником на имя руководителя ИТ-подразделения и утверждается руководителем структурного подразделения или ответственным должностным лицом, назначенные приказом Статкомитета СНГ.

Доступ к информации, содержащейся в базах данных Системы, сотрудников взаимодействующих, в том числе контролирующих, организаций осуществляется на основании заявки, утвержденной руководителем Статкомитета СНГ.

Сотруднику предоставляется индивидуальная учетная запись пользователя и временный пароль.

Бланк с учетными данными и уведомлением о смене временного пароля сотрудник получает под подпись у администратора баз данных. Первый вход в БД Системы пользователь осуществляет с временным паролем, производит замену временного пароля на основной и в дальнейшем доступ к ресурсам БД Системы осуществляет с основным паролем (известным только ему).

При выборе пароля необходимо руководствоваться требованиями к паролям, изложенными в разделе 4 «Требования к паролям».

Восстановление утерянного (забытого) пароля пользователя осуществляется администратором баз данных путем изменения (сброса) основного пароля пользователя. Основанием для изменения пароля является письменное уведомление пользователя на имя руководителя ИТ-подразделения. Устное заявление пользователя не является основанием для восстановления, утерянного пароля.

Администратор баз данных устанавливает временный пароль и опцию, требующую смены пароля пользователем. Регистрацию в БД Системы и создание основного пароля пользователь осуществляет с временным паролем, предоставленным администратором баз данных. Об изменении пароля администратор баз данных оповещает администратора информационной безопасности.

Для предотвращения подбора паролей администратор баз данных обязан настроить механизм блокировки учётной записи. Разблокирование учётной записи пользователя осуществляется администратором баз данных на основании служебной записки руководителя соответствующего структурного подразделения.

4. ТРЕБОВАНИЯ К ПАРОЛЯМ

В Статкомитете СНГ утверждены требования по организации парольной защиты.

Пароли не должны состоять из:

- имени, отчества или фамилии сотрудника Статкомитета СНГ;
- ими учётной записи (логина) ни в каком виде;
- другой информации о сотруднике (например, номера телефона и др.);
- только цифр или одинаковых букв;
- меньше чем из шести символов.

Пароли должны:

- содержать строчные и прописные буквы;
- содержать небуквенные символы (цифры, знаки пунктуации, специальные символы);
- быть легко запоминаемыми, чтобы не было необходимости их записывать;
- быть составлены так, чтобы сотрудник Статкомитета СНГ мог быстро набрать их на клавиатуре, что осложняет возможность подсмотреть пароль.

Владельцы паролей должны быть ознакомлены под роспись с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям.

Приложение № 3

УТВЕРЖДЕНО
приказом Статкомитета СНГ
от « 03 » 02 2020 г. № 5

**ИНСТРУКЦИЯ
ПО ОРГАНИЗАЦИИ АНТИВИРУСНОЙ ЗАЩИТЫ
В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ
СТАТКОМИТЕТА СНГ**

2020

1. ОБЩИЕ ПОЛОЖЕНИЯ

Антивирусная программа (антивирус) — любая программа для обнаружения компьютерных вирусов, а также нежелательных (считающихся вредоносными) программ вообще и восстановления зараженных (модифицированных) такими программами файлов, а также для профилактики — предотвращения заражения (модификации) файлов или операционной системы вредоносным кодом.

К использованию на компьютерах сотрудников допускаются только лицензионные антивирусные средства.

Установка и настройка средств антивирусной защиты на компьютерах осуществляются сотрудниками отдела информационных технологий.

Обновление средств антивирусного контроля осуществляется автоматически при подключении к сети Интернет.

2. ПРИМЕНЕНИЕ СРЕДСТВ АНТИВИРУСНОГО КОНТРОЛЯ

Средства антивирусного контроля работают в автоматическом режиме и не требуют от сотрудников никаких дополнительных действий. При обнаружении вируса на компьютере зараженный файл автоматически лечится, при невозможности лечения перемещается в специальный каталог (карантин). Администраторы получают извещение об обнаруженном вирусе и, при необходимости, предпринимают необходимые действия.

На компьютерах, подключенных к электронной почте, запрещается открывать вложенные файлы и запускать программы, полученные от неизвестного отправителя.

Установка (изменение) системного и прикладного программного обеспечения осуществляется сотрудником отдела информационных технологий. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено на отсутствие вирусов. Непосредственно после установки (изменения) программного обеспечения должна быть выполнена антивирусная проверка. Кроме того, устанавливаемое (изменяемое) программное обеспечение должно быть лицензионным, приобретенным через официальных дилеров фирм-разработчиков.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.) сотрудник структурного подразделения самостоятельно или вместе с сотрудником отдела информационных технологий должен провести внеочередной антивирусный контроль компьютера.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

- совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования;
- в случае обнаружения нового вируса, не поддающегося лечению применяемыми антивирусными средствами, сообщить об этом в отдел информационных технологий для дальнейшей передачи его в организацию, с которой заключен договор на антивирусную поддержку.

3. ОТВЕТСТВЕННОСТЬ

Ответственность за проведение мероприятий антивирусного контроля в локальной вычислительной сети Статкомитета СНГ и контроль над соблюдением

требований настоящей инструкции возлагается на администратора информационной безопасности и отдел информационных технологий.

Периодический контроль над состоянием антивирусной защиты в локальной вычислительной сети Статкомитета СНГ и на автономных автоматизированных рабочих местах сотрудников, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей инструкции возлагается отдел информационных технологий Статкомитета СНГ.

УТВЕРЖДЕНО
приказом Статкомитета СНГ
от « 03 » 02 2020 г. № 5

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА БАЗЫ ДАННЫХ ЛОКАЛЬНОЙ
ВЫЧИСЛИТЕЛЬНОЙ СЕТИ СТАТКОМИТЕТА СНГ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция определяет функциональные обязанности, права и ответственность администратора базы данных (далее — БД) локальной вычислительной сети Статкомитета СНГ по обеспечению безопасности информации.

Администратор БД назначается и освобождается от выполнения обязанностей приказом Статкомитета СНГ.

Администратор БД назначается из числа сотрудников отдела информационных технологий.

Непосредственное руководство администратором БД осуществляет начальник отдела информационных технологий.

В своей деятельности администратор БД руководствуется следующими документами:

- руководящими документами и указаниями по защите информации;
- документацией и рекомендациями производителей БД;
- должностной инструкцией.

2. ЗАДАЧИ АДМИНИСТРАТОРА БД

Основной задачей администратора БД является поддержание в актуальном рабочем состоянии полного объема информации, содержащейся в БД Системы, обеспечение защиты ее от хищения, утраты, утечки, уничтожения, искажения, подделки и блокирования доступа при ее обработке и хранении за счет несанкционированного доступа и специальных воздействий.

Администратор БД должен знать:

- руководящие и нормативные материалы, касающиеся управления базами данных, методов хранения, обработки и архивирования информации;
- руководящие и нормативные материалы, касающиеся организации вычислительных систем и использования вычислительной техники при обработке информации в Статкомитете СНГ;
- методы и средства контроля информации баз данных Системы, подлежащей защите, выявления каналов утечки информации.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА БД

Ознакомление сотрудников с перечнем сведений конфиденциального характера Статкомитета СНГ (совместно с администратором информационной безопасности).

Реализация разрешительной системы допуска пользователей к информации и связанным с ее использованием работам (совместно с администратором информационной безопасности).

Ограничение доступа персонала и посторонних лиц в помещение программно-аппаратного комплекса (ПАК ИАП, Система), где размещены средства информатизации и коммуникационное оборудование.

Разграничение доступа пользователей к информационным ресурсам Системы, программным средствам обработки (передачи) и защиты.

Регистрация действий пользователей Системы, контроль несанкционированного доступа и действий пользователей и посторонних лиц (совместно с администратором информационной безопасности).

Учет и надежное хранение носителей конфиденциальной информации, исключающее хищение, подмену и уничтожение.

Предотвращение внедрения в Систему программ-вирусов и программных закладок.

Контроль за размещением средств отображения информации, исключающее ее несанкционированный просмотр.

Своевременный анализ журнала учета событий с целью выявления возможных нарушений. Запрещение работы на рабочих станциях и серверах Системы посторонних лиц.

Осуществление периодических контрольных проверок рабочих станций и тестирование правильности функционирования средств защиты Системы (совместно с администратором информационной безопасности).

Администратору БД запрещается оставлять свою рабочую станцию без контроля, в том числе в рабочем состоянии.

Запрещается фиксировать учетные данные пользователя (пароли, идентификаторы, ключи и др.) на твердых носителях, а также сообщать их кому бы то ни было, кроме самого пользователя.

Сообщение информационной системе субъектами доступа своих имен (идентификация) и проверка подлинности (аутентификация) субъектов доступа при обращении к базе данных по идентификаторам (именам пользователей) и паролям длиной не менее восьми буквенно-цифровых символов.

Контроль доступа субъектов к БД в соответствии с правилами разграничения доступа.

Наблюдение за созданием и изменением БД, регистрация и протоколирование.

Регистрация входа (выхода) субъектов доступа в базу данных (из базы данных): регистрация выхода из базы данных не проводится в моменты аппаратурного отключения Системы. В параметрах регистрации указываются:

- дата и время входа (выхода) субъекта доступа в базу данных (из базы данных)
- результат попытки входа: успешная или неуспешная – несанкционированная;
- идентификатор (код или имя пользователя) субъекта, предъявленный при попытке доступа.

Регистрации вывода печатных документов и экспорта в файлы информации, отнесенной к разряду персональных данных.

В параметрах регистрации указываются:

- дата и время выдачи (обращение к подсистеме вывода);
- спецификация устройства выдачи (печатающее устройство, вывод в файл);
- краткое содержание (наименование документа и экранной формы, из которой производится печать документа или экспорт данных);
- идентификатор субъекта доступа, запросившего документ (имя пользователя и его IP-адрес);
- объем фактически выданного документа (количество страниц, листов, записей) и результат выдачи: успешный (весь объем), неуспешный.

Регистрация изменений полномочий субъектов доступа и статуса объектов доступа.

В параметрах регистрации указываются:

- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего измене-

Администратор БД ведет учет предоставленных прав доступа к информации, содержащейся в базах данных, в матрице доступа.

Администратор БД обязан производить административные действия со строго определенных доверенных станций, оснащенных средствами защиты от несанкционированного доступа.

4. ПРАВА АДМИНИСТРАТОРА БД

Для осуществления своей деятельности администратор БД имеет право доступа во все помещения, где установлены средства автоматизированной обработки информации.

Администратор БД имеет право прекращать автоматизированную обработку информации при наличии или угрозе утечки защищаемой информации.

Решение задач, связанных с организацией и управлением доступом пользователей к БД осуществляется администратором БД совместно с администратором информационной безопасности.

Ответственность за сохранность файлов БД несет администратор БД.

При контактах с пользователем решение об идентификации обратившегося лица администратор БД принимает любым доступным для него способом.

Все журналы и документы по безопасности администратор БД хранит на бумажном носителе не менее трех лет и при наличии их в электронном виде не менее года.

5. ТРЕБОВАНИЯ К РАБОЧЕЙ СТАНЦИИ И ИНСТРУМЕНТАЛЬНЫМ СРЕДСТВАМ АДМИНИСТРАТОРА БД

Рабочая станция администратора БД должна представлять собой специально выделенную для администратора ПЭВМ, которая является пунктом управления и контроля уровня защиты Системы и ее ресурсов.

Инструментальные средства, установленные на рабочей станции администратора БД (программные, программно-аппаратные, аппаратные), должны позволять эффективно решать задачи, поставленные перед ним.

6. ДЕЙСТВИЯ АДМИНИСТРАТОРА БД ПРИ ОБНАРУЖЕНИИ ПОПЫТОК НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К БД СИСТЕМЫ

К попыткам несанкционированного доступа (далее – НСД) относятся:

- сеансы работы с БД Системы незарегистрированных пользователей, пользователей, нарушивших установленную периодичность доступа, либо срок действия полномочий которых истек, либо в состав полномочий которых не входят операции по доступу к данным или манипулирования ими;

- действия третьего лица, пытающегося получить доступ (или получившего доступ) к БД Системы, при использовании учетной записи администратора или другого пользователя, в целях получения коммерческой или иной личной выгоды, методом подбора пароля или другого метода (компрометации пароля и т.п.).

При выявлении факта НСД администратор БД обязан:

- прекратить доступ к БД Системы со стороны выявленного участка НСД;
- доложить руководству Статкомитета СНГ служебной запиской о факте НСД, его результате (успешный, неуспешный) и предпринятых действиях;
- известить начальника структурного подразделения, в котором работает пользователь, от имени учетной записи которого была осуществлена попытка НСД, о факте НСД;
- поставить в известность администратора информационной безопасности и совместно проанализировать характер НСД.

Приложение № 5

УТВЕРЖДЕНО
приказом Статкомитета СНГ
от « 03 » 02 2020 г. № 5

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ
СТАТКОМИТЕТА СНГ

2020

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция определяет функциональные обязанности, права и ответственность администратора локальной вычислительной сети (далее – ЛВС) по обеспечению безопасности информации.

Администратор ЛВС назначается и освобождается от выполнения обязанностей приказом Председателя Статкомитета СНГ.

Администратор ЛВС назначается из числа сотрудников отдела информационных технологий.

Непосредственное руководство администратором ЛВС осуществляет начальник отдела информационных технологий.

В своей деятельности администратор ЛВС руководствуется следующими документами:

- руководящими документами по защите конфиденциальной информации и обеспечению информационной безопасности;
- должностной инструкцией.

2. ОСНОВНЫЕ ЗАДАЧИ АДМИНИСТРАТОРА ЛВС

Основными задачами администратора ЛВС являются:

- поддержка бесперебойного функционирования Информационно-телекоммуникационной системы Статкомитета СНГ и целостности базы данных;
- защита ЛВС от несанкционированного доступа, регулирование прав доступа пользователей сети к ресурсам ЛВС.
- обеспечение защиты информации ИТС Статкомитета СНГ от утечки по техническим каналам связи при ее обработке, хранении и передаче.

Администратор ЛВС должен знать:

- руководящие и нормативные материалы, касающиеся управления базами данных, методов хранения, обработки и архивирования информации;
- руководящие и нормативные материалы, касающиеся организации вычислительных систем и использования вычислительной техники при обработке информации в Статкомитете СНГ;
- методы защиты информации в локальных вычислительных сетях, выявления каналов утечки информации.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА ЛВС

Администратор ЛВС самостоятельно работает на основе уверенного знания основных параметров, требований, правил установки, способов выявления и устранения неполадок сетевых операционных систем и пользовательских сред, умеет квалифицированно работать с ними.

Устанавливает на серверы, рабочие станции и персональные компьютеры пользовательские и сетевые программы.

Конфигурирует и оптимизирует сеть и серверы с учетом рекомендаций отдела информационных технологий, разрабатывает и вносит на рассмотрение своего непосредственного руководителя предложения по оптимизации и развитию сети, в том числе по приобретению оборудования.

Обеспечивает бесперебойную работу серверов, сети и персональных компьютеров. Поддерживает рабочее состояние программного обеспечения серверов, рабочих станций, персональных компьютеров пользователей, подключенных и неподключенных к сети, принтеров, в том числе разрабатывает и реализует систему профилактических мер.

Обеспечивает интегрирование программного обеспечения управления базами и потоками данных сервера и рабочих станций.

Обеспечивает сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных).

Самостоятельно устраняет неполадки в работе программного обеспечения сети, серверов, персональных компьютеров.

В случае невозможности устранения неполадок в работе компьютеров, сервера, сети своими силами – привлекает специалистов сервисных организаций для устранения неисправностей сетевого оборудования. При этом активно участвует в восстановлении работоспособности указанных систем.

Обучает пользователей работе в сети; консультирует пользователей по вопросам использования программ, сети; составляет инструкции по работе с сетевым обеспечением и доводит их до сведения пользователей.

Обеспечивает ведение и актуализацию актов установленного программного обеспечения на рабочие станции пользователей, оформляет иную техническую документацию.

Принимает исчерпывающие меры по сохранению данных, в том числе в случае возникновения неполадок в сети, на серверах, в отдельных компьютерах, в том числе обеспечивает своевременное копирование и резервирование данных.

Контролирует использование сетевых ресурсов и дискового пространства, выявляет ошибки пользователей и неполадки сетевого программного обеспечения. Проводит разъяснительную работу. Сообщает своему непосредственному руководителю о случаях злоупотребления сетью и принятых мерах.

Участвует в разработке исходных данных и постановке задач на модернизацию компьютерной сети.

Разрабатывает способы и методы организации доступа пользователей компьютерной сети к ресурсам компьютерной сети.

Предотвращает несанкционированные модификации программного обеспечения, добавления новых функций, несанкционированный доступ к информации, аппаратуре и другим общим ресурсам компьютерной сети. В случае обнаружения модификаций или нерегламентированного программного обеспечения фиксирует событие в журнале учета обнаружения нерегламентированного программного обеспечения, ставит в известность руководителя структурного подразделения, где произошло событие, администратора информационной безопасности и совместно с ним проводит соответствующее расследование.

Администратор ЛВС должен осуществлять указанные ниже программно-технические сервисы безопасности:

- Идентификация и аутентификация субъектов доступа. Управление доступом к защищаемым ресурсам.
- Сообщение информационной системе субъектами доступа своих имен (идентификация) и проверка подлинности (аутентификация) субъектов доступа при входе в систему по идентификаторам (именам пользователей) и паролям длиной не менее восьми буквенно-цифровых символов.
- Идентификация серверов, рабочих станций, каналов связи, внешних устройств серверов и рабочих станций по логическим именам и (или) адресам.
- Контроль доступа субъектов к защищаемым ресурсам в соответствии с правилами разграничения доступа.
- Наблюдение за созданием и изменением объектов (файлов, каталогов, томов, серверов, рабочих станций, принтеров, каналов связи, внешних устройств серверов и рабочих станций), регистрация и протоколирование.

3.1 Регистрация запуска (завершения) программ и процессов

Под программами и процессами понимаются в том числе задания, задачи, предназначенные для обработки защищаемых файлов.

В параметрах регистрации указываются:

- дата и время запуска;
- идентификатор субъекта доступа, запросившего программу (процесс, задание);
- результат запуска (успешный, неуспешный, несанкционированный).
- регистрация попыток доступа программных средств к защищаемым файлам.

3.2 Регистрация попыток доступа программных средств к защищаемым файлам

Под программными средствами понимаются программы, процессы, задачи, задания

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла;
- имя программы (процесса, задания, задачи), осуществляющей доступ к файлу;
- вид запрашиваемой операции (чтение, запись, удаление, выполнение, расширение и т. п.).

3.3 Регистрация попыток доступа программных средств к защищаемым объектам

Под защищаемыми объектами понимаются серверы, рабочие станции, каналы связи, внешние устройства серверов и рабочих станций программам, тома, каталоги, файлы, записи, поля записей.

В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием результата регистрации: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта (логическое имя [номер]);
- имя программы (процесса, задания, задачи), осуществляющей доступ к защищаемому объекту;
- вид запрашиваемой операции (чтение, запись, монтирование, захват и т.п.).

3.4 Регистрация изменений полномочий субъектов доступа и статуса объектов доступа

В параметрах регистрации указываются:

- дата и время изменения полномочий;
- идентификатор субъекта доступа (администратора), осуществившего изменения.

Администратор ЛВС ведет учет предоставленных прав к иным информационным ресурсам в матрице доступа.

Администратор ЛВС обязан производить административные действия со строго определенных доверенных станций, оснащенных средствами защиты от несанкционированного доступа.

4. ПРАВА АДМИНИСТРАТОРА ЛВС

Для осуществления своей деятельности администратор ЛВС имеет право доступа во все помещения, где установлены средства автоматизированной обработки информации.

Администратор ЛВС имеет право прекращать автоматизированную обработку информации при наличии или угрозе утечки защищаемой информации.

Решение задач, связанных с организацией и управлением доступом пользователей к ресурсам ЛВС осуществляется администратором ЛВС совместно с администратором информационной безопасности и администратором баз данных.

При контактах с пользователем решение об идентификации обратившегося лица администратор ЛВС принимает любым доступным для него способом.

Все журналы и документы по безопасности администратор ЛВС хранит в электронном виде не менее трех лет, если иное не указано в технологической схеме.

УТВЕРЖДЕНО

приказом Статкомитета СНГ

от « 03 » 02 2020 г. № 5

ИНСТРУКЦИЯ
АДМИНИСТРАТОРА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ СТАТКОМИТЕТА СНГ

1. ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая инструкция определяет функциональные обязанности, права и ответственность администратора информационной безопасности (далее по тексту – администратор ИБ).

Администратор ИБ назначается и освобождается от выполнения обязанностей приказом председателя Статкомитета СНГ.

Администратор ИБ назначается из числа сотрудников отдела информационных технологий.

Непосредственное руководство администратором ИБ осуществляет начальник отдела информационных технологий.

2. ЗАДАЧИ АДМИНИСТРАТОРА ИБ

Основными задачами администратора ИБ является:

- организация эксплуатации технических и программных средств защиты информации;
- текущий контроль работы средств и систем защиты информации;
- обеспечение защиты информации Статкомитета СНГ от попыток несанкционированного доступа.

Администратор ИБ должен знать:

- руководящие и нормативные материалы, касающиеся управления защиты информации;
- руководящие и нормативные материалы, касающиеся организации вычислительных систем и использования вычислительной техники при обработке информации в Статкомитете СНГ;
- методы защиты информации в локальных вычислительных сетях (далее по тексту – ЛВС), выявления попыток несанкционированного доступа;
- принципы работы и администрирования технических и программных средств защиты информации в ЛВС.

3. ОБЯЗАННОСТИ АДМИНИСТРАТОРА ИБ

Администратор ИБ должен:

- знать перечень установленных в Статкомитете СНГ рабочих станций (АРМ) и перечень задач, решаемых с их использованием;
- осуществлять оперативный контроль за работой пользователей персональных компьютеров, анализировать содержимое системных журналов всех персональных компьютеров и адекватно реагировать на возникающие нештатные ситуации;
- осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых на компьютерах Статкомитета СНГ специальных технических средств защиты от несанкционированного доступа;
 - присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств персональных компьютеров и серверов, устанавливать и осуществлять настройку средств защиты персональных компьютеров;
 - периодически проверять состояние используемых средств защиты информации на АРМ пользователей, осуществлять проверку правильности их настройки (выборочное тестирование);

- докладывать начальнику отдела информационных технологий об имевших место попытках несанкционированного доступа к информации и техническим средствам АРМ;
- проводить занятия с сотрудниками по правилам работы на АРМ и по изучению руководящих документов по вопросам обеспечения безопасности информации;
- участвовать в расследовании причин совершения нарушений и возникновения серьезных кризисных ситуаций в результате несанкционированного доступа;
- конфигурировать и оптимизировать систему антивирусной с учетом рекомендаций отдела информационных технологий Статкомитета СНГ, разрабатывать и вносить на рассмотрение своего непосредственного руководителя предложения по оптимизации системы защиты информации;
- совместно с администратором ЛВС обеспечивать сетевую безопасность (защиту от несанкционированного доступа к информации, просмотра или изменения системных файлов и данных);
- обеспечивать автоматическую проверку (один раз в неделю) на наличие вирусов, с удалением обнаруженных, на всех объектах вычислительной техники, подключенных к ЛВС;
- соблюдать требования режима конфиденциальности информации, ставшей ему известной в связи с исполнением своих должностных обязанностей, и не использовать ее в интересах, не связанных с исполнением указанных обязанностей;
- осуществлять учет и периодический контроль действий администраторов ЛВС и БД, касающихся обеспечения информационной безопасности.

4. ПРАВА АДМИНИСТРАТОРА ИБ

Для осуществления своей деятельности администратор ИБ имеет право доступа во все помещения, где установлены средства автоматизированной обработки информации.

Администратор ИБ имеет право прекращать автоматизированную обработку информации при наличии или угрозе утечки защищаемой информации.

Решение задач, связанных с организацией и управлением доступом пользователей к ресурсам ЛВС осуществляется администратором ИБ совместно с администратором ЛВС и администратором баз данных.

Администратор ИБ имеет право проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов автоматизированной системы.

Администратор ИБ имеет право непосредственно обращаться к руководителям отделов с требованием прекращения работы в автоматизированной системе при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

Приложение № 7

УТВЕРЖДЕНО

приказом Статкомитета СНГ

от « 03 » 02 2020 г. № 5

**ИНСТРУКЦИЯ
ПОЛЬЗОВАТЕЛЯ ПЕРСОНАЛЬНОГО КОМПЬЮТЕРА
ПРИ РАБОТЕ В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ
СТАТКОМИТЕТА СНГ**

Настоящая инструкция устанавливает порядок работы сотрудников Статкомитета СНГ на персональных компьютерах в составе локальной вычислительной сети (ЛВС).

В инструкции описываются правила использования информации, циркулирующей в ЛВС, определения правил разграничения доступа к информации пользователей и содержатся необходимые требования по обеспечению совместной работы.

1. ОБЩИЕ ПОЛОЖЕНИЯ

Все компьютеры, подключенные к ЛВС, являются пользователями ее ресурсов. Каждый персональный компьютер имеет пользователя, который является ответственным за работоспособность и безопасность компьютера, и за соблюдение всех политик и процедур, связанных с использованием данного компьютера. На одном персональном компьютере допускается работа нескольких пользователей, но в этом случае один из них назначается основным пользователем.

До начала работы на персональном компьютере пользователи должны пройти обучение и изучить необходимые руководящие документы так, чтобы они могли корректно соблюдать все политики и процедуры. Обучение компьютерной безопасности проводится в рамках существующих программ обучения и курсов обучения, связанных с использованием информационных технологий.

Каждому пользователю назначается уникальный идентификатор пользователя (так называемая учетная запись пользователя) и начальный пароль. Пользователи не должны совместно использовать назначенные им идентификаторы.

Идентификатор пользователя изменяется и/или удаляется в соответствии с правилами, изложенными в «Порядке работы в корпоративной вычислительной сети Статкомитета СНГ».

Пользователю компьютера следует внимательно относиться к своим действиям, не ущемляя прав других пользователей и не препятствуя работе других компьютеров в сети.

Пользователь несет личную ответственность за весь информационный обмен между его компьютером и другими компьютерами в ЛВС и за ее пределами. В случае, если с персонального компьютера производился несанкционированный доступ к информации на других компьютерах, и в случаях других серьезных нарушений правил пользования сетью, по решению администратора ЛВС учетная запись пользователя данного компьютера отключается от сети, а непосредственно к пользователю, по результатам служебного расследования, применяются административные или другие меры воздействия.

Пользователи должны уважать права других пользователей на конфиденциальность и право на пользование общими ресурсами.

Для предотвращения распространения злонамеренного программного обеспечения и для выполнения лицензионных соглашений об использовании программ, пользователи должны гарантировать, что их программное обеспечение должным образом лицензировано и является безопасным. Сотрудникам отдела информационных технологий вменяется в обязанности производить периодический контроль над программным обеспечением, используемым на персональных компьютерах. Контроль производится негласно, результаты контроля и предлагаемые решения доводятся до сведения руководителей подразделений для принятия решения.

При использовании персонального компьютера в составе ЛВС пользователю запрещается:

- получать доступ к конфиденциальной информации без разрешения ее собственника;
- повреждение, уничтожение или фальсификация доступной служебной информации;

- совершать попытки обхода системы авторизации доступа в ЛВС, ее повреждение или дезинформация;
- распространять информацию, запрещенную к распространению действующим законодательством, а также информацию, не соответствующую морально-этическим нормам ее получателей, а также производить рассылку рекламных, обманных, беспокоящих или угрожающих сообщений внутри ЛВС и за ее пределы;
- использовать ресурсы ЛВС без разрешения на использование этих ресурсов.
- использовать предоставленные ресурсы в целях, отличных от тех, для которых они (ресурсы) предоставлены данному пользователю;
- устанавливать и использовать различные компьютерные программы, не предназначенные к использованию на данном рабочем месте (персональном компьютере);
- изменять настройку общесистемного программного обеспечения компьютера;
- вскрывать корпус компьютера;
- передавать свой пароль другим пользователям, хранить его в общедоступном месте.

2. ПОСЛЕДОВАТЕЛЬНОСТЬ ДЕЙСТВИЙ, НЕОБХОДИМЫХ ДЛЯ ПОЛУЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИ, НАХОДЯЩЕЙСЯ В ЛВС

Включить компьютер и/или монитор. После загрузки системы на экране компьютера появится окно авторизации. Необходимо ввести пароль, полученный от сотрудника отдела информационных технологий.

Название учетной записи пользователя (идентификатор пользователя) и пароль пользователя чувствительны к регистру, т.е. операционная система воспримет «ПАРОЛЬ», «пароль» или «Пароль» как совершенно разные значения. При этом Вы не сможете видеть набираемые символы, т.к. они будут отображаться в виде звездочек "*****".

После ввода имени пользователя и пароля необходимо нажать клавишу "ENTER". Если пароль был введен правильно, то начнет выполняться системная процедура регистрации в сети, которая автоматически подключит доступные для Вас ресурсы на сервере. Вам необходимо дождаться конца ее выполнения.

Если вы ошиблись в наборе имени пользователя или пароля следует набрать имя пользователя и пароль снова. Рекомендуется обратить внимание, символами какого языка набирается пароль.

Для выхода из сети без выключения компьютера, следует совершить последовательность действий: "Пуск/ Завершение работы / Завершение сеанса <идентификатор пользователя>".

Для выхода из сети с выключением компьютера, следует совершить последовательность действий: "Пуск/ Завершение работы / Завершение работы" и дождаться выключения компьютера или появления на экране сообщения «Теперь можно выключить питание компьютера».

Современные компьютеры имеют возможность «засыпать», т.е. снижать энергопотребление до минимума, в случае их длительного (настраиваемый параметр, обычно несколько десятков минут) простоя. Для увеличения ресурса работоспособности персональных компьютеров, в случае, когда он подключен к электрической сети через источник бесперебойного питания, управляемый ОС компьютера. При этом необходимо выключать только монитор персонального компьютера, а системный блок оставлять включенным. О наличии такой возможности в каждом конкретном случае необходимо справиться у сотрудников отдела информационных технологий.

В любом случае, для сохранения ресурсов работоспособности аккумуляторных батарей источника бесперебойного питания, запрещается его физическое отключение от сети электроснабжения, даже в случае длительного отсутствия пользователя.

3. ЧТО ПРОИСХОДИТ ПОСЛЕ ВХОДА В ИНФОРМАЦИОННУЮ СЕТЬ

После входа в сеть, на компьютере проходит процедура регистрации, во время которой обновляется необходимое программное обеспечение, включая антивирусное, подключаются сетевые диски, необходимые для работы и запускаются программы, находящиеся в папке «Автозагрузка». Рекомендуется дождаться завершения запуска всех программ и только после этого приступать к работе.

За создание и актуализацию резервных копий важной, конфиденциальной или персональной информации, хранящейся на персональном компьютере, несет ответственность сам пользователь.

При возникновении у пользователя подозрений о несанкционированном доступе к его персональному компьютеру он обязан немедленно, любым доступным способом, поставить в известность сотрудников отдела информационных технологий и действовать строго в соответствии с полученными от них указаниями, не предпринимая никаких самостоятельных действий.

4. УСТРАНЕНИЕ НЕИСПРАВНОСТЕЙ КОМПЬЮТЕРНОЙ ТЕХНИКИ

Пользователю категорически запрещается вскрывать корпус персонального компьютера и заниматься самостоятельным изменением конфигурации его аппаратной части.

При обнаружении каких-либо неисправностей в работе компьютерной техники или ЛВС или их нештатной работы, необходимо:

- не предпринимать никаких самостоятельных действий для устранения возникших неполадок, в том числе не закрывать возникшие сообщения об ошибках при их появлении;
- при наличии возможности – произвести копирование важной служебной и личной информации в домашний каталог пользователя;
- обратиться любым доступным способом в отдел информационных технологий и четко сформулировать возникшую проблему;
- действовать в соответствии с указаниями, полученными от сотрудников отдела информационных технологий.

5. РЕКОМЕНДАЦИИ ПО ИСПОЛЬЗОВАНИЮ ПАРОЛЯ

Порядок использования пароля сотрудниками Статкомитета СНГ должен соответствовать требованиям Инструкции по организации парольной защиты в локальной вычислительной сети Статкомитета СНГ.

Приложение № 8

УТВЕРЖДЕНО
приказом Статкомитета СНГ
от « 03 » 02 2020 г. № 5

**ИНСТРУКЦИЯ
ПО ПОРЯДКУ РЕЗЕРВИРОВАНИЯ, ХРАНЕНИЯ И УНИЧТОЖЕНИЯ
МАССИВОВ И НОСИТЕЛЕЙ ИНФОРМАЦИИ В
СТАТКОМИТЕТЕ СНГ**

2020

1. НАЗНАЧЕНИЕ И ОБЛАСТЬ ДЕЙСТВИЯ ИНСТРУКЦИИ

Настоящая инструкция по порядку резервирования, хранения и уничтожения массивов и носителей информации (далее – Инструкция) разработана для регламентации действий сотрудников, ответственных за резервирование, хранение и уничтожение массивов и носителей информации.

Область действия Инструкции – Статкомитет СНГ.

Сотрудник Статкомитета СНГ, допущенный к работе с информацией, должен быть под подпись ознакомлен с требованиями настоящей Инструкции и ответственностью за ее нарушение.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Порядок хранения, выдачи и уничтожения массивов и носителей информации вводится, изменяется и контролируется структурным подразделением Статкомитета СНГ, ответственным за защиту информации.

Резервирование служебной информации, размещенной в Программно-аппаратном комплексе «Информационно-аналитический веб-портал Статкомитета СНГ» Информационно-телекоммуникационной системы Статкомитета СНГ (далее ПАК ИАП, Система), производится ответственным сотрудником, назначенным распоряжением руководителя подразделения Статкомитета СНГ.

3. ПОРЯДОК СОЗДАНИЯ, УЧЕТА, РЕГИСТРАЦИИ И ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ БД

Все операции копирования на внешние носители информации и их удаления выполняются администратором баз данных или администратором ЛВС.

Резервирование и хранение программного обеспечения и баз данных Системы осуществляется в соответствии с приказами Статкомитета СНГ.

Все операции копирования архивов на внешние носители информации, а также их удаления регистрируются в «Журнале учета носителей информации с резервными копиями базы данных Системы».

Все операции автоматизированного копирования и удаления архивов регистрируются в соответствующих файлах электронных журналов. Контроль за выполнением регламентных работ и автоматизированным резервным копированием производится администратором баз данных.

Детальное описание порядка создания резервной копии базы данных **consstat** Системы приведено в разделе 4 документа «Информационно-телекоммуникационная система Статкомитета СНГ. Программно-аппаратный комплекс "Информационно-аналитический веб-портал Статкомитета СНГ". Руководство системного администратора» (18398612.00004156.001001.ИЗ.02).

4. ПОРЯДОК СОЗДАНИЯ, УЧЕТА, РЕГИСТРАЦИИ И ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ КОНТЕНТА ВЕБ-ПОРТАЛА

Все операции по созданию, учету, регистрации и хранению резервных копий контента веб-портала выполняются администратором баз данных или администратором ЛВС.

Все операции копирования контента на внешние носители информации, а также их удаления регистрируются в «Журнале учета носителей информации с резервными

копиями контента веб-портала».

Все операции автоматизированного копирования и удаления контента веб-портала регистрируются в соответствующих файлах электронных журналов. Контроль за выполнением регламентных работ и автоматизированным резервным копированием производится администратором баз данных.

Детальное описание порядка создания резервной копии контента веб-портала ИТС Статкомитета СНГ приведено в разделе 4 документа «Информационно-телекоммуникационная система Статкомитета СНГ. Программно-аппаратный комплекс "Информационно-аналитический веб-портал Статкомитета СНГ". Руководство системного администратора» (18398612.00004156.001001.ИЗ.02).

5. ПОРЯДОК СОЗДАНИЯ, УЧЕТА, РЕГИСТРАЦИИ И ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ ВИРТУАЛЬНОЙ ИНФРАСТРУКТУРЫ ПАК ИАП

Все операции по созданию, учету, регистрации и хранению резервных копий виртуальной инфраструктуры ПАК ИАП выполняются администратором локально-вычислительной сети (ЛВС).

Ежедневная резервная копия виртуального сервера Базы данных (БД) Системы хранится в течение 41 дня на дисковом пространстве системы хранения данных.

Еженедельная резервная копия виртуальной инфраструктуры ПАК ИАП хранится в течение 8 недель на дисковом пространстве системы хранения данных.

Ежемесячная резервная копия виртуальной инфраструктуры ПАК ИАП хранится в течение 6 месяцев на дисковом пространстве системы хранения данных.

Ежегодная резервная копия виртуальной инфраструктуры ПАК ИАП хранится в течение 5 лет на дисковом пространстве системы хранения данных.

Все операции автоматизированного копирования и удаления виртуальной инфраструктуры регистрируются в соответствующих файлах электронных журналов. Контроль за выполнением регламентных работ и автоматизированным резервным копированием производится администратором ЛВС.

Детальное описание порядка создания резервной копии виртуальной инфраструктуры ИТС Статкомитета СНГ приведено в подразделе 4.5 документа «Информационно-телекоммуникационная система Статкомитета СНГ. Программно-аппаратный комплекс "Информационно-аналитический веб-портал Статкомитета СНГ". Руководство системного администратора» (18398612.00004156.001001.ИЗ.02).

6. ПОРЯДОК ОБРАЩЕНИЯ НОСИТЕЛЕЙ И АРМ С ИНФОРМАЦИЕЙ БД ЗА ПРЕДЕЛАМИ СТАТКОМИТЕТА СНГ

Для обработки информации БД Системы с использованием сменных носителей информации сотрудник Статкомитета СНГ обязан заранее представить «Разрешение на использование базы данных Системы за пределами административного Статкомитета СНГ» (далее – Разрешение), утвержденное руководителем структурного подразделения.

В Разрешении должно быть указано:

- дата получения носителя;
- ФИО и должность сотрудника, кому передается носитель;
- место временной работы с БД за пределами Статкомитета СНГ;
- цель работы.

Разрешение должно быть подписано руководителем структурного подразделения Статкомитета СНГ, которому выдается информация БД Системы.

После получения Разрешения, администратор информационной системы устанавливает необходимые обновления программного обеспечения, базы данных, проводит проверку на наличие вирусной активности сменного носителя и выдает носитель ответственному сотруднику Статкомитета СНГ, указанному в Разрешении. После этого ответственный сотрудник имеет право хранить, использовать и модифицировать информацию, содержащуюся на носителе. При этом считается, что информация БД может находиться на носителях.

7. РЕГИСТРАЦИЯ НОСИТЕЛЕЙ И ЖУРНАЛА УЧЕТА НОСИТЕЛЕЙ

Все сменные носители информации Статкомитета СНГ, используемые при обработке конфиденциальной информации, подлежат регистрации и обязательному учету.

Носитель информации, который принимается на учет, подвергается проверке на предмет его годности, целостности и работоспособности. Например, сменные жесткие диски проверяются на штатном сервере с использованием соответствующих утилит ОС, оптические диски проверяются визуально, flash-память проверяется на компьютере сотрудника и т. д.

Годному к использованию носителю информации сотрудником ИТ-отдела, назначенному приказом руководителя Статкомитета СНГ ответственным за обращение носителей, присваивается учетный номер носителя и делается регистрационная запись с использованием «Журнала учета носителей служебной информации».

На носитель информации любым доступным способом в удобном для просмотра месте проставляется учетный номер носителя (наклейка, надпись и т.п.), пометка "Для служебного пользования".

В «Журнале учета носителей служебной информации» делается запись о приемке на учет носителя. При этом заполняются графы:

- регистрационный номер, наименование носителя;
- ФИО, должность исполнителя;
- действие по учету носителя;
- дата;
- подпись лица, получившего носитель.

Страницы журнала нумеруются, прошиваются, скрепляются печатью. Ответственность за ведение «Журнала учета носителей информации» возлагается на сотрудника профильного подразделения.

Учет носителей, содержащих конфиденциальную информацию, имеет следующие особенности:

- учетные носители информации передаются сотрудникам Статкомитета СНГ под подпись в «Журнале учета съемных носителей служебной информации».
- в «Журнале учета съемных носителей служебной информации» делается запись о получении, передаче или возврате носителя.

При этом заполняются графы:

- регистрационный номер, наименование носителя;
- ФИО, должность исполнителя;
- действие по учету носителя;
- дата;
- подпись лица, получившего носитель.

Страницы журнала нумеруются, прошиваются, скрепляются печатью. Ответственность за ведение «Журнала учета носителей информации» возлагается на сотрудника профильного подразделения.

8. ПОРЯДОК СОЗДАНИЯ, УЧЕТА, РЕГИСТРАЦИИ ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ ПРОЧИХ ИР СТАТКОМИТЕТА СНГ

Резервные копии прочих информационных ресурсов (ИР) Статкомитета СНГ создаются лицами, ответственным за их состояние.

Сроки создания резервных копий информационных ресурсов (подсистем, баз данных, файлов) Статкомитета СНГ, сроки хранения резервных копий устанавливаются:

- регламентами эксплуатации соответствующих ИР Статкомитета СНГ;
- приказами руководителей Статкомитета СНГ;
- распоряжениями ИТ-отдела.

Для учета, регистрации и хранения резервных копий ИР, содержащихся на серверах Системы, ведётся «Журнал учета резервных копий ИР». Страницы «Журнала учета резервных копий ИР» нумеруются, прошиваются, скрепляются печатью.

Факт создания резервной копии ИР регистрируется записью в «Журнале учета резервных копий ИР». Сотрудник подразделения, ответственный за создание резервных копий ИР, после изготовления резервной копии обязан:

- зарегистрировать сделанную копию ИР в «Журнале учета резервных копий ИР» (с указанием регистрационного номера сменного носителя);
- передать резервную копию ИР, с отметкой о сдаче в «Журнале учета резервных копий ИР», руководителю подразделения для хранения в сейфе;
- при создании резервной копии ИР с использованием программ архивирования, применяемый при этой процедуре, пароль должен быть записан и, в запечатанном конверте, передан руководителю подразделения для хранения в сейфе.

9. УЧЕТ МАШИННЫХ СЪЕМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

Съемные машинные носители информации (флэш-накопители, оптические диски и т.д.), предназначенные для хранения информации, учитываются по «Журналу учета носителей служебной информации» сотрудником, отвечающим за обеспечение выполнения в Статкомитете СНГ предусмотренных мер защиты информации.

На съемных машинных носителях информации любым доступным способом в удобном для просмотра месте проставляются следующие учетные реквизиты: учетный номер и дата выдачи, пометка «Для служебного пользования», подпись сотрудника, отвечающего за обеспечение выполнения в Статкомитете СНГ предусмотренных мер защиты информации.

Учетные машинные носители информации передаются сотрудникам Статкомитета СНГ под подпись в журнале учета носителей служебной информации.

Машинные носители информации, пришедшие в негодность, неисправные или потерявшие практическую ценность, уничтожаются по акту.

10. ПРАВИЛА РАБОТЫ И ОБЯЗАННОСТИ ДОЛЖНОСТНЫХ ЛИЦ ПО ПРОЦЕДУРЕ РЕЗЕРВИРОВАНИЯ СЛУЖЕБНОЙ ИНФОРМАЦИИ, ЕЕ ХРАНЕНИЮ И УНИЧТОЖЕНИЮ

Категорически запрещается копирование и обработка любой информации, переносимой с помощью сменных носителей, без производственной необходимости.

Категорически запрещается производить резервирование информации на неучтенные носители.

Носители, предназначенные для хранения копий, пришедшие в негодность, снимаются с эксплуатации путем физического разрушения (разлома или разрезания).

Уничтожение информации производится ответственным сотрудником Статкомитета СНГ в присутствии администратора информационной безопасности, о чём производится соответствующая запись в «Журнале учета носителей резервных копий служебной информации» или в «Журнале учета носителей резервных копий ИР» за тремя подписями: администратора информационной безопасности, ответственного сотрудника Статкомитета СНГ и ответственного за резервирование служебной информации подразделения.

Все факты разрушения данных на рабочих станциях, классифицируются как «значимые нарушения информационной безопасности» и должны анализироваться через процедуру служебного расследования.

11. ТРЕБОВАНИЯ К ОБОРУДОВАНИЮ ПОМЕЩЕНИЙ ДЛЯ ХРАНЕНИЯ РЕЗЕРВНЫХ КОПИЙ ИНФОРМАЦИИ

К оборудованию помещений для хранения резервных копий информации предъявляются следующие требования:

- помещение должно оборудоваться сейфом, или металлическим хранилищем, имеющим резервные ключи и устройства для опечатывания;
- помещения и оборудование размещены таким образом, чтобы исключить возможность бесконтрольного проникновения в эти помещения посторонних лиц;
- контроль над входом в помещение регистратора служащими службы охраны, осуществляющими наружную охрану;
- должностное лицо, осуществляющее хранение резервных копий, должно иметь печать для опечатывания сейфа или металлического хранилища;
- хранение резервных электронных копий баз данных должно осуществляться в месте, отвечающем требованиям сохранности и конфиденциальности.

12. ОТВЕТСТВЕННЫЕ ЛИЦА

Ответственность за резервирование информационных ресурсов (ИР) и служебной информации и ведение «Журнала учета резервных копий информационных ресурсов» возлагается на ответственного сотрудника, назначенного распоряжением руководителя подразделения.

Ответственность за ведение «Журнала учета носителей служебной информации» и «Журнала учета сменных носителей служебной информации» возлагается на администратора информационной безопасности, назначенного распоряжением руководителя подразделения.

Контроль за соблюдением правильности политики резервирования данных и учета носителей информации, предназначенных для создания резервных копий служебной информации, возлагается на администратора информационной безопасности.

Ответственность за ввод в действие, установку и обновление необходимого программно-аппаратного обеспечения технологии резервирования данных возлагается на администратора баз данных объекта информатизации.

Ответственность за своевременное уничтожение пришедших в негодность носителей резервных копий несут ответственные за резервирование информации сотрудник подразделения и администратор информационной безопасности.

13. ЗАМЕНА НЕИСПРАВНЫХ НОСИТЕЛЕЙ, СОДЕРЖАЩИХ КОНФИДЕНЦИАЛЬНУЮ ИНФОРМАЦИЮ, В СЕРВИСНОЙ СЛУЖБЕ

Для замены неисправного носителя выполняются следующие действия:

- представителями Статкомитета СНГ и сервисной службы составляется двусторонний акт о неисправности носителя;
- представитель Статкомитета СНГ временно снимает носитель с эксплуатации с записью в «Журнале учета носителей служебной информации», отсоединяет от носителя и передает в сервисную службу блок электроники носителя;
- представитель сервисной службы передает по акту новый носитель представителю Статкомитета СНГ;
- представитель Статкомитета СНГ устанавливает новый носитель, осуществляет настройку сервера или Системы хранения данных (СХД), регистрирует новый носитель в соответствии с разделом 7 настоящей инструкции.

14. УНИЧТОЖЕНИЕ МАССИВОВ И НОСИТЕЛЕЙ ИНФОРМАЦИИ

Ненужные для дальнейшего использования массивы информации, пришедшие в негодность, неисправные или потерявшие практическую ценность, снимаются с эксплуатации и уничтожаются по акту путем стирания файлов.

Уничтожение носителя производится администратором информационной безопасности (ИБ), о чём производится соответствующая запись в «Журнале учета носителей служебной информации» за тремя подписями: администратора ИБ, ответственного сотрудника структурного подразделения и сотрудника профильного подразделения, назначенного приказом Статкомитета СНГ, ответственным за учет носителей.

Приложение № 9

УТВЕРЖДЕНО
приказом Статкомитета СНГ
от « 03 » 02 2020 г. № 5

ТЕХНОЛОГИЯ
БЕСПРОВОДНЫХ КОММУНИКАЦИЙ В ЛОКАЛЬНОЙ
ВЫЧИСЛИТЕЛЬНОЙ СЕТИ СТАТКОМИТЕТА СНГ

2020

1. ЦЕЛИ ТЕХНОЛОГИИ

Технология беспроводных коммуникации (далее – Технология) разработана и утверждена в целях определения технических и организационных критериев, требований и правил использования технологий беспроводного доступа в Статкомитете СНГ.

Настоящая Технология является методологической основой практических мер по обеспечению информационной безопасности в Статкомитете СНГ при использовании беспроводных коммуникаций.

Положения и требования данного документа распространяются на все структурные подразделения Статкомитета СНГ.

Положения Технологии также распространяются на все сторонние организации и учреждения, взаимодействующие со Статкомитете СНГ в качестве поставщиков и потребителей информационных ресурсов в том или ином качестве.

2. НОРМАТИВНЫЕ ССЫЛКИ

NIST Special Publication 800-48 Wireless Network Security for IEEE 802.11a/b/g and Bluetooth;
NIST Special Publication 800-97 Establishing Wireless Robust Security Networks.

3. ОБЩИЕ ПОЛОЖЕНИЯ

Действие настоящей Технологии распространяется на все устройства, поддерживающие технологии беспроводного доступа и передачи информации, находящиеся и функционирующие в рамках локальной вычислительной сети (ЛВС) Статкомитета СНГ.

Беспроводные сети и устройства, находящиеся вне ЛВС Статкомитета СНГ, и не имеющие никакого с ней соединения, под действие настоящей Технологии не подпадают.

Требованиями настоящей Технологии запрещается без разрешения и соответствующих настроек средств защиты на них подключать устройства беспроводного доступа к локально-вычислительным сетям Статкомитета СНГ (включая средства беспроводного доступа, размещенные на ноутбуках, сотовых телефонах и других мобильных устройствах).

Все устройства беспроводного доступа (включая клиентские) до ввода в эксплуатацию должны быть учтены и настроены уполномоченными сотрудниками отдела информационных технологий с учетом требований настоящей Технологии.

Ввод в эксплуатацию каждого устройства беспроводного доступа должен быть согласован с отделом информационных технологий.

Клиентские беспроводные устройства сторонних лиц и организаций разрешается подключать к точкам беспроводного доступа Статкомитета СНГ, реализующим доступ только к общедоступной сети Интернет по согласованию с отделом информационных технологий. Их подключение осуществляется после выполнения процедур учета, получения разрешения на эксплуатацию и настройки в соответствии с настоящей Технологией.

4. ТОЧКИ БЕСПРОВОДНОГО ДОСТУПА

Настоящая Технология задает следующие требования по организации точек беспроводного доступа Статкомитета СНГ:

- в обязательном порядке логин и пароль для администрирования точки доступа, установленные по умолчанию, должны быть изменены;

- для административного доступа к точке доступа должны использоваться протоколы SNMPv3 и/или SSL/TLS в случае использования веб-интерфейса управления;
- необходимо, чтобы у сети был задан уникальный SSID;
- необходимо обеспечить шифрование потока данных;
- необходимо обеспечить, чтобы сигнал точки доступа минимально выходил за пределы физически контролируемого периметра;
- на точке доступа должно осуществляться ведение журналов аудита и их постоянный анализ.

5. ТРЕБОВАНИЯ К КЛИЕНТАМ

На всех беспроводных устройствах, с использованием которых пользователи получают доступ к ЛВС Статкомитета СНГ, должны соблюдаться следующие требования:

- клиентские беспроводные устройства доступа должны соответствовать требованиям Инструкции по антивирусной защите в локальной вычислительной сети Статкомитета СНГ;
- на клиентских беспроводных устройствах должны быть активированы встроенные в операционные системы или антивирусное программное обеспечение или средства межсетевого экранирования;
- на клиентских устройствах доступа к беспроводной сети не должно содержаться публичных ресурсов.

6. РАСПРЕДЕЛЕНИЕ ОТВЕТСТВЕННОСТИ

В сферу ответственности Руководства Статкомитета СНГ входит обеспечение необходимого ресурсного обеспечения деятельности в области обеспечения безопасности беспроводных сетей Статкомитета СНГ.

В сферу ответственности отдела информационных технологий входит:

- совершенствование схем организации подключения точек предоставления беспроводного доступа;
- настройка устройств беспроводного доступа;
- поддержание в работоспособном состоянии устройств беспроводного доступа;
- регистрация и учет устройств беспроводного доступа;
- периодическая проверка отсутствия несанкционированных подключений средств беспроводного доступа к сети Статкомитета СНГ и настроек средств защиты устройств беспроводного доступа.

7. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящая Технология вступает в силу с момента её утверждения приказом Председателя Статкомитета СНГ.

Решения о внесении изменений и дополнений в Технологию, а также о признании части или всех её положений утратившими силу утверждаются приказом Председателя Статкомитета СНГ.

Все изменения и дополнения в содержание Технологии фиксируются в листе регистрации изменений новой редакции. Новая редакция Технологии утверждается приказом Председателя Статкомитета СНГ.

Ответственным за пересмотр и актуализацию настоящей Технологии является начальник отдела информационных технологий Статкомитета СНГ .

Приложение № 10

УТВЕРЖДЕНО

приказом Статкомитета СНГ

от « 03 » 02 2020 г. № 5

**ПОРЯДОК
ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТЫ
В СТАТКОМИТЕТЕ СНГ**

2020

1. ЦЕЛИ ПОРЯДКА

Порядок использования электронной почты в Статкомитете СНГ (далее – Порядок) является документом, разработанным в целях:

- задания принципов и правил использования сервиса электронной почты.
- определения ответственности и обязанностей пользователей сервиса электронной почты, а также информирования пользователей о допустимом и недопустимом использовании сервиса.

Настоящий Порядок является методологической основой практических мер по обеспечению информационной безопасности Статкомитета СНГ при использовании электронной почты.

Положения и требования данного документа распространяются на все структурные подразделения Статкомитета СНГ.

Положения Порядка также распространяются на все сторонние организации и учреждения, взаимодействующие со Статкомитетом СНГ в качестве поставщиков и потребителей информационных ресурсов Статкомитета СНГ в том или ином качестве.

Действие настоящего Порядка распространяются на:

- пользователей Статкомитета СНГ;
- администраторов сервиса электронной почты Статкомитета СНГ;
- сотрудников отдела информационных технологий Статкомитета СНГ.

2. ОБЩИЕ ПОЛОЖЕНИЯ

Электронная почта – один из наиболее широко используемых видов обмена электронными сообщениями, который является не просто способом доставки сообщений, а важнейшим средством коммуникации, распределения информации и управления различными процессами. Роль электронной почты становится очевидной, если рассмотреть функции, которые выполняет почта:

- обеспечивает внутренний и внешний информационный обмен;
- является компонентом системы документооборота.

Благодаря выполнению этих функций электронная почта решает одну из важнейших на настоящий момент задач – формирует единое информационное пространство Статкомитета СНГ.

Риски, связанные с использованием электронной почты:

- рассылка спама;
- вероятный канал утечки конфиденциальной информации при отсутствии должного контроля (возможность пересылки разных форматов документов);
- распространение вредоносного программного обеспечения.

3. ИСПОЛЬЗОВАНИЕ СЕРВИСА ЭЛЕКТРОННОЙ ПОЧТЫ

К входящим и исходящим сообщениям электронной почты должны быть разработаны требования безопасности. Данные требования должны быть документированы.

В целях сокращения непроизводительных потерь времени при работе с сервисом электронной почты Статкомитета СНГ и уменьшения информационных рисков, должна в обязательном порядке производиться проверка всех сообщений на соответствие разработанным требованиям безопасности.

Сообщения электронной почты должны проходить следующие обязательные проверки:

- проверка сообщений на наличие вредоносного программного обеспечения;
- проверка сообщений на наличие спама;
- контентный анализ сообщений на соответствие требованиям безопасности.

В целях осуществления контентного анализа должно использоваться специализированное программное обеспечение (система контроля содержимого электронной почты (content security software)). Данное программное обеспечение должно обеспечивать:

- проведение текстового анализа;
 - фильтрацию передаваемых данных по размеру и объему данных, по количеству вложений в сообщения электронной почты, по типу файлов (вложенных в электронную почту), по адресу электронной почты;
 - контроль использования почтовых ресурсов и разграничение доступа к ним различных категорий пользователей;
 - отложенную доставку сообщений электронной почты по расписанию;
 - ведение полнофункционального архива электронной почты.
- разбора сообщений электронной почты на составляющие компоненты с последующим анализом их содержимого);
- рекурсивную декомпозицию (специальный алгоритм, применяемый для разбора сообщений электронной почты на составляющие компоненты с последующим анализом их содержимого);
 - эвристическое определение кодировок текстов;
 - определение типа файлов по сигнатуре;
 - полнотекстовый поиск по архиву электронной почты и т.п.

4. ПРАВА ВЛАДЕНИЯ

Все сообщения, хранящиеся в системе электронной почты Статкомитета СНГ, включая все почтовые вложения, являются информацией, принадлежащей Статкомитету СНГ.

5. СФЕРЫ ОТВЕТСТВЕННОСТИ

В сферу ответственности пользователей Статкомитета СНГ входит:

- ознакомление под роспись с правилами использования сервиса электронной почты, утвержденными в Статкомитете СНГ;
- знание и соблюдение установленных правил использования сервиса электронной почты Статкомитета СНГ;
- своевременное оповещение сотрудников отдела информационных технологий и администраторов сервиса электронной почты о фактах нарушения требований настоящего Порядка (например, о получении спама и т.п.);
- своевременное удаление неактуальных электронных сообщений (сообщения, полученные по ошибке, спам и т.п.);
- использование сервиса электронной почты исключительно для выполнения трудовых обязанностей.

Ответственность администраторов сервиса электронной почты.

В сферу ответственности администраторов сервиса электронной почты входит:

- выполнение задач администрирования сервиса электронной почты Статкомитета СНГ;

- обеспечение резервного копирования почтовых ящиков пользователей в соответствии с установленными регламентами;
- восстановление удаленных писем из резервной копии;
- обеспечение гарантированного уровня обслуживания по предоставлению почтового сервиса;
- поддержание в работоспособном состоянии систем защиты электронной почты Статкомитета СНГ.

6. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящий Порядок вступает в силу с момента её утверждения приказом Председателя Статкомитета СНГ.

Решения о внесении изменений и дополнений в Порядок, а также о признании части или всех её положений утратившими силу, утверждаются приказом Председателя Статкомитета СНГ.

Все изменения и дополнения в содержание Порядка фиксируются в листе регистрации изменений новой редакции. Новая редакция Порядка утверждается приказом Председателя Статкомитета СНГ.

Ответственным за пересмотр и актуализацию настоящего Порядка является начальник отдела информационных технологий Статкомитета СНГ .

Приложение № 11

УТВЕРЖДЕНО
приказом Статкомитета СНГ
от « 03 » 02 2020 г. № 5

**ПОРЯДОК
ПО КОНТРОЛЮ И АНАЛИЗУ ЗАЩИЩЕННОСТИ
ИНФОРМАЦИОННЫХ РЕСУРСОВ СТАТКОМИТЕТА СНГ**

2020

1. ЦЕЛИ ПОРЯДКА

Порядок по контролю и анализу защищенности информационных ресурсов Статкомитета СНГ (далее – Порядок) разработан в целях обеспечения на необходимом уровне детализации целей, задан и порядка реализации требований в Статкомитете СНГ к проведению контроля и инструментального анализа защищенности информационных ресурсов.

Настоящий Порядок является методологической основой практических мер по обеспечению информационной безопасности Статкомитета СНГ.

Положения и требования данного документа распространяются на все структурные подразделения Статкомитета СНГ.

Положения Порядка также распространяются на все сторонние организации и учреждения, взаимодействующие со Статкомитетом СНГ в качестве поставщиков и потребителей информационных ресурсов Статкомитета СНГ в том или ином качестве.

2. ОСНОВНЫЕ ПРИНЦИПЫ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ

Контроль и анализ защищенности информационных ресурсов в Статкомитете СНГ должен проводиться на регулярной основе, в целях обнаружения существующих уязвимостей информационных систем Статкомитета СНГ.

В рамках контроля и анализа защищенности информационных ресурсов должны охватываться следующие компоненты информационных систем:

- системное и прикладное программное обеспечение (ПО) серверов и рабочих станций;
- ПО систем управления базами данных (СУБД);
- телекоммуникационное оборудование;
- программное и аппаратное обеспечение средств защиты информации (СЗИ).

Причины обнаруженных уязвимостей должны оперативно анализироваться с целью их скорейшего устранения.

Для каждой информационной системы из состава информационных ресурсов Статкомитета СНГ должны быть назначены сотрудники, ответственные за разбор (анализ) и устранение уязвимостей.

Результаты каждой из проверок защищенности информационных ресурсов должны сохраняться для использования в последующих аудитах информационной безопасности.

3. ТРЕБОВАНИЯ К КОНТРОЛЮ ЗАЩИЩЕННОСТИ

В части обеспечения контроля наличия уязвимостей в программном обеспечении, операционных системах, сетевых сервисах и СУБД должно быть обеспечено:

- выявление известных ошибок в программном обеспечении операционных систем серверов информационных ресурсов Статкомитета СНГ используемых ими сетевых сервисов и СУБД;
- выявление известных ошибок в программном обеспечении общесистемного прикладного ПО;
- выявление известных ошибок в реализации ПО сетевых служб, протоколов и СУБД;
- выявление известных ошибок в реализации сетевых служб и протоколов;

- контроль своевременной установки пакетов с исправлениями и обновлений программного обеспечения;
- выявление настроек «по умолчанию» (не измененных после инсталляции стандартных настроек систем, которые могут быть использованы для осуществления несанкционированного доступа);
- выявление слабых (легкоугадываемых) паролей;
- выявление несоблюдения требований по обеспечению контроля действий пользователей (при наличии аудита), отсутствия регистрации действий пользователей.

Хранилище событийной информации, а также средства управления системой контроля защищенности, должны быть защищены от вмешательства и несанкционированного доступа.

Информация о действиях операторов и администраторов средств системы контроля защищенности должна записываться в журнал событий.

Используемые средства контроля защищенности не должны значительно снижать производительность компонентов информационных ресурсов Статкомитета СНГ.

4. СФЕРА ОТВЕТСТВЕННОСТИ

В сферу ответственности сотрудников отдела информационных технологий входит:

- участие в проектировании средств контроля защищенности информационных ресурсов;
- помощь в реализации задач по внедрению и настройке средств контроля защищенности информационных ресурсов;
- участие в развитии, сопровождении и контроле состояния инфраструктуры средств контроля защищенности информационных ресурсов;
- обслуживание и администрирование средств контроля защищенности информационных ресурсов;
- участие в проведении служебных расследований причин нарушения настоящей Политики.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящий Порядок вступает в силу с момента её утверждения приказом Председателя Статкомитета СНГ.

Решения о внесении изменений и дополнений в Порядок, а также о признании части или всех её положений утратившими силу утверждаются приказом Председателя Статкомитета СНГ.

Все изменения и дополнения в содержание Порядка фиксируются в листе регистрации изменений новой редакции. Новая редакция Порядка утверждается приказом Председателя Статкомитета СНГ.

Ответственным за пересмотр и актуализацию настоящего Порядка является начальник отдела информационных технологий Статкомитета СНГ.

УТВЕРЖДЕНО
приказом Статкомитета СНГ
от « 03 » 02 2020 г. № 5

**РЕКОМЕНДАЦИИ
ПО ФИЗИЧЕСКОЙ ЗАЩИТЕ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ
СТАТКОМИТЕТА СНГ**

1. ЦЕЛИ РЕКОМЕНДАЦИЙ

Рекомендации по физической защите объектов информатизации Статкомитета СНГ (далее – Рекомендации) является документом, разработанным в целях:

- обеспечения на необходимом уровне детализации целей, задач и порядка реализации требований в Статкомитете СНГ к обеспечению мер физической защиты объектов информатизации;

- определения ответственности структурных подразделений Статкомитета СНГ за разработку и внедрение мер физической защиты объектов информатизации.

Положения и требования данного документа распространяются на все структурные подразделения Статкомитета СНГ.

2. НОРМАТИВНЫЕ ССЫЛКИ

ГОСТ Р 51275-2006. «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения».

3. ОРГАНИЗАЦИОННЫЕ И ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ И ОГРАНИЧЕНИЯ

3.1 Периметр физической безопасности

Физическая защита объектов информатизации должна быть основана на определенных периметрах безопасности и обеспечиваться путем установки в Статкомитете СНГ ряда барьеров, расположенных в стратегических местах. Требования к каждому защитному барьеру и его месторасположению должны определяться ценностью активов, подлежащих защите, а также рисками нарушения безопасности и существующими защитными мерами. Каждый уровень физической защиты должен иметь определенный периметр безопасности, в пределах которого должен быть обеспечен надлежащий уровень защиты.

При организации защищенных физических периметров требуется обеспечить следующие меры:

- периметр безопасности должен соответствовать ценности защищаемых ресурсов и сервисов;
- периметр безопасности должен быть четко определен;
- вспомогательное оборудование (например, фотокопировальные аппараты, факс-машины) должны быть размещены так, чтобы уменьшить риск несанкционированного доступа или компрометации конфиденциальной информации;

- физические барьеры должны по необходимости простираться от пола до потолка, чтобы предотвратить несанкционированный доступ в помещение;

- посторонние лица не должны иметь информацию о том, что делается в защищенных областях;

- должны быть обеспечена возможность установления запрета на работу в одиночку без надлежащего контроля; это необходимо как для безопасности, так и для предотвращения потенциальных вредоносных действий;

- вычислительная техника и оборудование, принадлежащее Статкомитету СНГ, должно размещаться в специально предназначенных для этого местах, отдельно от оборудования, контролируемого сторонними организациями;

- в нерабочее время защищенные области должны быть физически недоступны (закрыты на замки) и периодически проверяться охраной;
- персоналу, осуществляющему техническое обслуживание сервисов, должен быть предоставлен доступ в защищенные области только в случае необходимости и только после получения необходимого разрешения. Доступ такого персонала (особенно к конфиденциальным данным) должен быть ограничен, а его действия должны быть под контролем;
- в пределах периметра безопасности использование фотографической, звукозаписывающей и видео аппаратуры должно быть запрещено, за исключением санкционированных случаев.

3.2 Контроль доступа в помещения

В защищенных областях требуется установить надлежащий контроль доступа в помещения, чтобы только персонал, имеющий соответствующие полномочия, имел к ним доступ. Должны быть обеспечены следующие меры контроля:

- за посетителями защищенных областей должен быть установлен надзор, а дата и время их входа и выхода должны регистрироваться; посетителям должен быть предоставлен доступ для конкретных, разрешенных целей;
- у сотрудников, увольняющихся с данного места работы, требуется немедленно изъять права доступа в защищенные области.

3.3 Защита центров данных и компьютерных залов

Центры обработки данных и компьютерные залы, поддерживающие критически важные сервисы Статкомитета СНГ, должны иметь надежную физическую защиту.

При выборе и обустройстве соответствующих помещений требуется учитывать возможность повреждения оборудования в результате пожара, наводнения, взрывов, гражданских беспорядков и других аварий. С этой целью должны быть определены угрозы безопасности, которые могут быть реализованы из соседних помещений.

Должны быть предусмотрены следующие меры:

- ключевые системы должны размещаться как можно дальше от общедоступных мест и мест прохождения общественного транспорта;
- здания не должны привлекать внимание и выдавать свое назначение (по возможности); не должно быть явных признаков как снаружи, так и внутри здания, указывающих на присутствие вычислительных ресурсов;
- внутренние телефонные справочники не должны указывать на местонахождение вычислительных ресурсов;
- установлено соответствующее сигнальное и защитное оборудование, например, тепловые и дымовые детекторы, пожарная сигнализация, средства пожаротушения, а также предусмотрены пожарные лестницы;
- сигнальное и защитное оборудование требуется регулярно проверять в соответствии с инструкциями производителей; сотрудники должны быть надлежащим образом подготовлены к использованию этого оборудования;
- процедуры реагирования на чрезвычайные ситуации должны быть полностью документированы и регулярно тестироваться.

3.4 Организация защищенных областей для критически важных или уязвимых сервисов Статкомитета СНГ

Информационные системы, поддерживающие критически важные или уязвимые сервисы Статкомитета СНГ, должны быть размещены в защищенных областях и должны быть также защищены физически от несанкционированного доступа, повреждения и помех. Защищенные области должны быть ограничены определенным периметром безопасности, с надлежащим контролем доступа в помещения и защитными барьерами.

3.5 Изолированные места разгрузки и загрузки оборудования и материалов

Помещения объектов информатизации, в которых размещены средства обработки информации должны быть защищены от несанкционированного доступа. Должны быть обеспечены следующие меры:

- доступ к складским помещениям снаружи здания должен предоставляться только проверенному персоналу, имеющему соответствующие полномочия;
- складское помещение должно быть спланировано так, чтобы материалы можно было разгружать без получения доступа в другие помещения здания;
- внешняя дверь в складское помещение должна быть заперта, когда открыта внутренняя дверь;
- требуется определить потенциальную опасность, которую могут представлять собой поступающие материалы, прежде чем их переместить из складского помещения в место назначения.

3.6 Применение средств физической защиты от пожаров, наводнений и других видов техногенных угроз

Для предотвращения ущерба от пожара, наводнения, землетрясения, взрыва, гражданских беспорядков и других подобных угроз необходимо рассмотреть следующие рекомендации:

- опасные и горючие материалы должны храниться на безопасном расстоянии от месторасположения вычислительных ресурсов;
- крупные партии канцелярской продукции (бумаги, печатной продукции и т.п.), не должны храниться внутри защищенных участков объектов информатизации;
- резервное оборудование и носители информации, на которых хранятся резервные копии, должны быть размещены на безопасном расстоянии, чтобы избежать их повреждения в случае аварии на основном рабочем месте;
- на объектах информатизации Статкомитета СНГ должно размещаться оборудование противопожарной защиты в соответствии с действующими противопожарными нормами.

3.7 Правила использования рабочего стола

В Статкомитете СНГ должны быть разработаны и утверждены правила использования рабочего стола, касающиеся документов и съёмных носителей информации, чтобы уменьшить риск несанкционированного доступа, потери и повреждения информации.

С этой целью должно быть обеспечено выполнение следующих требований:

- бумажная документация и съёмные носители информации, когда они не используются, должны храниться в сейфах (запираемых шкафах), особенно в нерабочее время;
- конфиденциальная или критически важная производственная информация, когда она не используется, должна храниться отдельно (лучше всего в несгораемом

шкафу), особенно в нерабочее время;

- персональные компьютеры и компьютерные терминалы, когда они не используются, должны быть защищены с помощью ключей, паролей или других средств контроля;

- должны быть установлены необходимые меры защиты входящей и исходящей почты, а также факсов, оставленных без присмотра.

4. ОРГАНИЗАЦИОННЫЕ МОМЕНТЫ И СТРУКТУРА ОТВЕТСТВЕННОСТИ

4.1 Общие требования по организации физической защиты

Для обеспечения физической защиты объектов информатизации должны быть выполнены следующие меры:

- организация периметра физической безопасности;
- контроль доступа в помещения;
- защита серверного помещения (термозоны);
- организация защищенных областей для критически важных или уязвимых сервисов Статкомитета СНГ;
- использование изолированных мест разгрузки и загрузки оборудования и материалов;
- применение средств физической защиты от пожаров, наводнений и других видов техногенных угроз;
- разработка и внедрение правил использования рабочего места.

4.2 Ответственность за реализацию требований, определённых настоящими Рекомендациями

Отдел информационных технологий отвечает за:

- планирование и управление требованиями по обеспечению физической защиты объектов информатизации Статкомитета СНГ;
- проектирование, внедрение, сопровождение и модернизацию механизмов физической защиты объектов информатизации;
- планирование и управление требованиями по обеспечению физической защиты объектов информатизации Статкомитета СНГ, участвующих в обработке конфиденциальной информации Статкомитета СНГ.

5. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

Настоящие Рекомендации вступают в силу с момента их утверждения приказом Председателя Статкомитета СНГ.

Решения о внесении изменений и дополнений в Рекомендации, а также о признании части или всех положений утратившими силу утверждаются приказом Председателя Статкомитета СНГ.

Все изменения и дополнения в содержание Рекомендаций фиксируются в листе регистрации изменений новой редакции. Новая редакция Рекомендаций утверждается приказом Председателя Статкомитета СНГ.

Ответственным за пересмотр и актуализацию настоящих Рекомендаций является начальник отдела информационных технологий Статкомитета СНГ.

Приложение № 13

УТВЕРЖДЕНО
приказом Статкомитета СНГ
от « 03 » 02 2020 г. № 5

**ПОЛОЖЕНИЕ
О КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ СТАТКОМИТЕТА СНГ**

2020

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Положение о конфиденциальной информации (далее – Положение) устанавливает порядок обращения с конфиденциальной информацией, являющейся собственностью Статкомитета СНГ, его контрагентов и определяет основные меры ее защиты вследствие неправомерного использования (утраты, хищения, разглашения или фальсификации).

1.2 Цель Положения – определение основных мер защиты конфиденциальной информации с целью предотвращения ее неправомерного использования (утраты, хищения, разглашения или фальсификации).

1.3 Положение является основополагающим нормативным документом, регламентирующим деятельность Статкомитета СНГ в сфере защиты конфиденциальной информации. Требования Положения обязательны для выполнения всеми сотрудниками Статкомитета СНГ.

1.4 Действие Положения не распространяется на устанавливаемый международными и государственными органами режим защиты сведений, составляющих государственную тайну.

1.5 Руководители структурных подразделений Статкомитета СНГ несут персональную ответственность за обеспечение режима соблюдения конфиденциальной информации на участке деятельности подразделения, организуют выполнение установленных Положением режимных требований, принимают меры по максимальному ограничению возможности ознакомления с информацией сотрудников, которым по роду выполняемых ими должностных обязанностей она не требуется.

1.6 В вопросах сохранения конфиденциальных сведений, предоставляемых Статкомитету СНГ контрагентами, следует руководствоваться действующим законодательством страны пребывания, Положением, а также условиями обеспечения охраны конфиденциальности, изложенными в соответствующих договорах и (или) соглашениях, заключенных с контрагентами.

1.7 Все структурные подразделения и сотрудники Статкомитета СНГ, контрагенты, допускаемые к конфиденциальным сведениям; лица, оказывающие Статкомитету СНГ услуги в соответствии с заключенными договорами возмездного оказания услуг, если эти услуги связаны с конфиденциальной информацией Статкомитета СНГ, являются пользователями Положения.

1.8 Права на документ принадлежат Статкомитету СНГ. Документ не может быть полностью или частично воспроизведен, опубликован, тиражирован, скопирован или распространен в любой иной форме без разрешения Статкомитета СНГ.

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

2.1 Термины и определения.

В Положении используются указанные ниже термины и определения.

Термин	Определение
Информация	Сведения (сообщения, данные), независимо от формы их представления.

Информационная безопасность	Состояние защищенности информационной среды Статкомитета СНГ, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств.
Документированная информация (документ)	- Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. - Зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или ее материальный носитель.
Конфиденциальная информация	Документированная информация, доступ к которой ограничивается. Информация, требующая защиты.
Информация (сведения), составляющая коммерческую тайну	Сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны.
Носители информации (сведений), составляющей коммерческую тайну	Материальные объекты, в том числе физические поля, в которых сведения, составляющие коммерческую тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.
Машинный носитель информации	Материальный носитель или устройство, предназначенное для записи, хранения и считывания информации средствами вычислительной и (или) оргтехники - персональными компьютерами (рабочими станциями), серверами и другими техническими средствами.
Энергонезависимый машинный носитель информации	Машинный носитель информации, информация в которых, в отличие от энергозависимых машинных носителей информации, сохраняется после отключения электропитания или их изъятия из устройств, в которые они устанавливаются.
Документ на машинном носителе (электронный документ)	Документ, созданный с использованием носителей и способов записи, обеспечивающих обработку его информации электронно-вычислительной машиной.
Гриф ограничения доступа к документу (ограничительный гриф)	Реквизит официального документа, свидетельствующий об особом характере информации, ограничивающий круг пользователей документом.

Разглашение информации	Несанкционированное доведение защищаемой информации до потребителей, не имеющих права доступа к этой информации.
Утрата конфиденциальных документов	Выход (в том числе и временный) документов из владения ответственного за их сохранность сотрудника, которому они были доверены, вследствие чего эти документы, а равно содержащиеся в них сведения, стали, либо могли стать достоянием посторонних лиц.
Защита информации	Организационные, правовые, технические и технологические меры по предотвращению угроз информационной безопасности и устранению их последствий.
Средства защиты информации	Технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих коммерческую тайну, и иных конфиденциальных сведений, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.
Обработка сведений (информации)	Получение, хранение, преобразование, комбинирование, передача или любое другое использование сведений (информации).
Контрагент	Сторона гражданско-правового договора, которой обладатель информации, составляющей коммерческую тайну, передал эту информацию.
Контрагент Статкомитета СНГ	Юридические и физические лица, с которыми взаимодействует Статкомитет СНГ при выполнении работ (оказании услуг) на основании заключенных договоров (соглашений, контрактов).
Информационные технологии	Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов.

2.2 Сокращения

В Положении применены указанные ниже сокращения:

Сокращение	Наименование сокращения
Статкомитет СНГ	Межгосударственный статистический комитет Содружества Независимых Государств
К	Гриф конфиденциальности – "Конфиденциально"

СВТ	Средства вычислительной техники
Перечень	Перечень конфиденциальных сведений Статкомитета СНГ
Положение	Положение о конфиденциальной информации Статкомитета СНГ

3. РЕЖИМ КОНФИДЕНЦИАЛЬНОСТИ СТАТКОМИТЕТА СНГ

3.1 Режим конфиденциальности в Статкомитете СНГ устанавливается в отношении конфиденциальной информации (сведений), обладателем которой являются Статкомитет СНГ, другие юридические и физические лица, если в заключенных с ними договорах (соглашениях) оговорена необходимость обеспечения охраны конфиденциальности таких сведений.

Режим конфиденциальности устанавливается:

а) в отношении информации, исключительным собственником которой является Статкомитет СНГ в соответствии с Положением, и разработанных на его основе других внутренних нормативных документов;

б) в отношении информации, собственниками которой являются другие юридические и физические лица, - в соответствии с договорами и (или) соглашениями с правообладателями этой информации;

в) в отношении персональных данных сотрудников Статкомитета СНГ, командированных лиц и посетителей – в соответствии с Положением;

г) в отношении иной информации ограниченного доступа – в соответствии с требованиями действующего законодательства страны пребывания.

3.2 Документированной конфиденциальной информации присваивается ограничительный гриф "Конфиденциально" ("К"). На материальных носителях с указанной документированной информацией наименование ее обладателя и его местоположение не проставляется.

4. ПОРЯДОК ОТНЕСЕНИЯ СВЕДЕНИЙ К КОНФИДЕНЦИАЛЬНЫМ, СНЯТИЯ ОГРАНИЧЕНИЙ НА РАСПРОСТРАНЕНИЕ СВЕДЕНИЙ

4.1 К сведениям конфиденциального характера относятся:

а) сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные), за исключением сведений, подлежащих распространению в средствах массовой информации в установленных законами страны пребывания случаях;

б) сведения, составляющие тайну следствия и судопроизводства, а также сведения о защищаемых лицах и мерах государственной защиты, осуществляемой в соответствии с нормативными правовыми актами страны пребывания;

в) служебные сведения, доступ к которым ограничен органами государственной власти и федеральными законами (служебная тайна) страны пребывания;

г) сведения, связанные с профессиональной деятельностью, доступ к которым ограничен законодательством страны (врачебная, нотариальная, адвокатская тайна, тайна

переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

д) сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них;

е) иные сведения, решение о конфиденциальности которых принято руководством Статкомитета СНГ.

4.2 Отнесение сведений к категории "Конфиденциально" производится:

а) в отношении информации, исключительным собственником которой является Статкомитет СНГ;

б) в отношении информации, собственниками которой являются другие юридические и физические лица, - в соответствии с договорами и (или) соглашениями с правообладателями этой информации.

4.3 Персональную ответственность за правильность определения степени конфиденциальности информации и своевременность проставления ограничительного грифа «К» на документах и иных материальных носителях несет исполнитель, а также лицо, подписывающее (утверждающее) документ.

4.4 Если по мнению исполнителя (лица, подписывающего документ), сведения должны быть отнесены к конфиденциальным, он представляет согласованные с руководителем подразделения аргументированные предложения в Управление делами Статкомитета СНГ об отнесении соответствующих сведений к конфиденциальным. До принятия решения защита указанных сведений должна быть обеспечена в соответствии с требованиями Положения.

4.5 Конфиденциальные сведения утрачивают необходимость защиты:

а) по соглашению заинтересованных сторон, установивших ограничения;

б) в случае принятия решения руководством Статкомитета СНГ об открытом соглашении сведений и после фактически состоявшегося соглашения.

4.6 Снятие ограничений на распространение конфиденциальных сведений производится по решению председателя Статкомитета СНГ на основании обоснованного представления структурного подразделения, являющегося владельцем сведений.

4.7 Снятие ограничений на распространение конфиденциальных сведений, которые являются результатом совместной деятельности Статкомитета СНГ и других юридических и физических лиц, допускается только по согласованию с ними.

4.8 О снятии ограничений на распространение конфиденциальных сведений Статкомитета СНГ, извещаются юридические и физические лица, которым эти сведения были переданы на договорных условиях.

5. ПОРЯДОК ДОПУСКА СОТРУДНИКОВ К КОНФИДЕНЦИАЛЬНЫМ СВЕДЕНИЯМ И ПРЕКРАЩЕНИЯ ДОПУСКА

5.1 Основанием для допуска сотрудников к конфиденциальным сведениям Статкомитета СНГ, является приказ о принятии на работу либо заключение договора гражданско-правового характера.

5.2 После издания приказа и до предоставления фактического доступа сотрудника к конфиденциальным сведениям, руководитель структурного подразделения, в которое поступает сотрудник:

- доводит до сотрудника под подпись требования Положения и Перечень конфиденциальных сведений Статкомитета СНГ, а также других документов, регламентирующих порядок работы с конфиденциальной информацией;

- предупреждает об ответственности за нарушение установленного в Статкомитете СНГ режима конфиденциальности;

- передает сотруднику копию Памятки по обеспечению сохранности конфиденциальных сведений Статкомитета СНГ.

5.3 Организация доступа сотрудника к информационным ресурсам электронных вычислительных систем Статкомитета СНГ осуществляется Информационно-издательским управлением Статкомитета СНГ.

5.4 Фактический доступ сотрудника к документам, машинным носителям и информационным ресурсам электронных вычислительных систем Статкомитета СНГ, содержащим конфиденциальные сведения, в объеме, необходимом для исполнения им должностных обязанностей, организует его непосредственный руководитель.

5.5 Обязанность сотрудника соблюдать требования настоящего Положения, а также ответственность за разглашение конфиденциальных сведений отражается в заключаемом с ним трудовом договоре.

5.6 Основанием для прекращения доступа к конфиденциальным сведениям является:

- приказ об увольнении сотрудника;
- заявление сотрудника об увольнении либо объявление сотруднику в соответствии с трудовым законодательством о предстоящем увольнении (в этом случае необходимость и объем работы с конфиденциальными документами на период до издания приказа определяет заместитель председателя Статкомитета СНГ по направлению деятельности);
- нарушение сотрудником взятых на себя обязательств, связанных с неразглашением конфиденциальных сведений;
- решение председателя Статкомитета СНГ об отстранении сотрудника от работы с конфиденциальными сведениями. Решение оформляется приказом и доводится до сведения сотрудника под роспись.

5.7 При наличии одного из перечисленных оснований непосредственный руководитель сотрудника, доступ которого к конфиденциальным сведениям прекращен, обязан незамедлительно сообщить об этом в Управление делами.

5.8 При увольнении сотрудника за допущенное нарушение трудовой дисциплины, своих обязательств по трудовому договору со Статкомитетом СНГ или в иных случаях, предусмотренных законодательством, Информационно-издательское управление принимает меры по ограничению доступа сотрудника к информационным ресурсам, содержащим конфиденциальную информацию.

6. ОБЯЗАННОСТИ СОТРУДНИКОВ, ДОПУЩЕННЫХ К КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

6.1 Сотрудники Статкомитета СНГ, допущенные к конфиденциальной информации, обязаны:

- знать и выполнять требования Положения и других нормативных документов Статкомитета СНГ, регламентирующих порядок обращения с конфиденциальной информацией;
- не разглашать конфиденциальную информацию, полученную в результате выполнения своих должностных обязанностей;
- соблюдать установленные в Статкомитете СНГ правила работы с документами, порядок их учета, хранения и уничтожения;
- знакомиться только с теми документами и информацией, к которым получили допуск в силу своих должностных обязанностей;
- во время работы с документами принимать меры к исключению возможности ознакомления с ними других лиц, не имеющих к ним прямого отношения;
- пресекать действия других лиц, которые могут привести к разглашению

конфиденциальных сведений;

- при составлении конфиденциальных документов ограничиваться минимальными, действительно необходимыми сведениями;

- определять количество экземпляров документа в строгом соответствии со служебной необходимостью;

- документы, содержащие конфиденциальные сведения и находящиеся на исполнении (не подшитые в дела), хранить в отдельной папке;

- в нерабочее время, а также при кратковременном отсутствии на рабочем месте документы, содержащие конфиденциальную информацию, хранить в закрытом на замок шкафу (сейфе);

- документы с грифом "К" после их исполнения группировать (подшивать) в дела, предусмотренные номенклатурой дел структурного подразделения, в соответствии с порядком, установленным в Статкомитете СНГ;

- немедленно информировать руководителя структурного подразделения и начальника Управления делами о фактах утраты (недостачи) документов (отдельных листов), содержащих конфиденциальную информацию, ключей от сейфов (шкафов), фактах обнаружения неучтенных конфиденциальных документов, а также о фактах необоснованного интереса к конфиденциальным сведениям со стороны лиц, не имеющих прямого отношения к работе с ними.

6.2 При обработке конфиденциальной информации с использованием средств вычислительной и оргтехники сотрудники обязаны:

- соблюдать правила разграничения доступа к охраняемым данным, неукоснительно выполнять требования нормативных документов по организации доступа к информационным ресурсам, организации парольной и антивирусной защиты;

- не разглашать свои индивидуальные пароли на доступ к компьютерным, сетевым и иным информационным ресурсам, выполнять требования соответствующих администраторов вычислительной сети и администраторов автоматизированных (информационных) систем по смене паролей, не применять "простых" паролей, не оставлять в легкодоступных местах листы и конверты с паролями;

- принимать меры к исключению ознакомления посторонних лиц с информацией, выводимой на экран дисплея;

- при подготовке электронных документов, содержащих конфиденциальную информацию, в верхнем правом углу (колонтитуле) первого экранного листа проставлять пометку с соответствующим ограничительным грифом ("Конфиденциально");

- не использовать (не загружать, не запускать и т.п.) для обработки конфиденциальной информации сторонние программные средства, не допущенные для применения в Статкомитете СНГ. При требовании операционной системы обновления установленного программного обеспечения обязательно его произвести;

- при необходимости покинуть свое рабочее место провести стандартные процедуры выхода из системы и отключения компьютера (в рабочее время допускается инициализация экранной заставки, защищенной индивидуальным паролем, или блокировка доступа к компьютеру с использованием аппаратно-программных средств и электронных ключей, принятых для эксплуатации в Статкомитете СНГ);

- не допускать случаев передачи конфиденциальной информации по незащищенным каналам передачи данных, через сеть Интернет и иные публичные сети (включая факс);

- не допускать случаев передачи конфиденциальной информации по электронной почте в открытом виде;

- в нерабочее время, а также при кратковременном отсутствии на рабочем месте хранить съемные машинные носители, содержащие конфиденциальные сведения, в закрытом на замок сейфе (шкафу);

- немедленно информировать руководителя структурного подразделения о фактах или возможности несанкционированного доступа к информации в локальной вычислительной сети (ЛВС) Статкомитета СНГ.

6.1. Сотрудникам, допущенным к конфиденциальной информации, запрещается:

- снимать и изготавливать копии конфиденциальных документов (в том числе с электронных документов), делать из них выписки без разрешения руководителя структурного подразделения;

- выносить за пределы здания Статкомитета СНГ документы и машинные носители с конфиденциальными сведениями без разрешения своего руководителя подразделения. В случае служебной необходимости выноса (вывоза) документов и носителей, содержащих конфиденциальную информацию, на срок командировки разрешение должно получаться у заместителя председателя или председателя Статкомитета СНГ. При этом в служебной записке указывается перечень документов (электронных документов на машинных носителях), отнесенных к конфиденциальным;

- работать с документами и иными материалами, содержащими конфиденциальные сведения, вне служебных помещений;

- обсуждать вопросы, содержащие конфиденциальные сведения в присутствии посторонних лиц;

- сообщать устно или письменно кому бы то ни было конфиденциальную информацию, если это не обусловлено выполнением служебных обязанностей.

6.1.1. Кроме того, сотрудникам Статкомитета СНГ запрещается:

- подключать к компьютерам различного рода внешние устройства, устанавливать на компьютеры и (или) использовать программные продукты (программы), копировать на (с) внешние машинные носители программное обеспечение без разрешения руководителя подразделения, за исключением программного обеспечения, устанавливаемого в соответствии с нормативными документами Статкомитета СНГ;

- самостоятельно, без разрешения руководителя подразделения, подключать (или допускать подключение) к ЛВС Статкомитета СНГ компьютеры (в том числе мобильные) представителей контрагентов и других организаций или физических лиц, прибывающих в Статкомитет СНГ;

- вносить без разрешения руководителя подразделения в пределы охраняемой территории Статкомитета СНГ и использовать без согласования для обработки служебной и конфиденциальной информации личные компьютеры (ноутбуки);

- использовать для сохранения информации, составляющей коммерческую тайну, личные (не принадлежащие Статкомитету СНГ) компьютеры (в том числе мобильные - ноутбуки, карманные персональные компьютеры (КПК), электронные записные книжки, смартфоны, мобильные телефоны и другие мобильные цифровые (вычислительные) устройства);

- использовать средства корпоративной электронной почты для отправки неслужебной корреспонденции, сообщать персональные электронные почтовые адреса для получения неслужебной корреспонденции (в том числе электронных рассылок) через сеть Интернет.

7. ОРГАНИЗАЦИЯ РАБОТЫ С КОНФИДЕНЦИАЛЬНЫМИ ДОКУМЕНТАМИ

7.1. Для всех структурных подразделений Статкомитета СНГ устанавливается единый порядок учета, хранения, размножения, рассылки и уничтожения документальных материалов, содержащих конфиденциальную информацию.

7.2. Работа с документами, содержащими конфиденциальную информацию, регламентируется нормативными документами Статкомитета СНГ по ведению конфиденциального делопроизводства.

8. ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ ПРИ ЕЕ ОБРАБОТКЕ НА СРЕДСТВАХ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

8.1. Сохранность конфиденциальной информации при ее обработке на средствах вычислительной техники (СВТ) и передаче по компьютерным сетям Статкомитета СНГ обеспечивается осуществлением комплекса организационных, технических и программных мер защиты информации.

8.2. Обязательными условиями обработки конфиденциальной информации на СВТ являются:

- персональный допуск пользователей к работе на СВТ в соответствии с установленным порядком;
- разграничение полномочий и доступа пользователей к информационным ресурсам автоматизированных и информационных систем корпоративной компьютерной сети (обеспечивается системными средствами разграничения, использованием индивидуальных идентификаторов и паролей, электронных ключей и т.п.);
- ведение учета всех электронных носителей конфиденциальной информации;
- обособленное хранение (в отдельных областях сетевых дисков, директориях, папках, файлах и т.п.) конфиденциальных сведений с максимально возможным разграничением по доступу;
- создание резервных копий информационных массивов;
- стирание по миновании практической надобности информации и проектов документов, содержащих конфиденциальную информацию, оставшихся на внешних запоминающих устройствах СВТ, а также очистка оперативной памяти путем выключения и перезагрузки компьютера после обработки конфиденциальной информации Статкомитета СНГ;
- уничтожение информации с машинных носителей (уничтожение машинных носителей информации), на которые осуществлялась запись конфиденциальной информации, в случае выхода их из строя или непригодности (нецелесообразности) для дальнейшего использования, а также при плановой или внеплановой замене СВТ, в том числе при обновлении парка компьютеров;
- отключение на компьютерах сотрудников Статкомитета СНГ внешних устройств записи информации (накопителей на гибких магнитных дисках (дискетах), приводов CD- RW, USB-портов и т.п. устройств записи информации). В случае производственной необходимости подключение таких устройств на компьютерах сотрудников, которые по роду исполнения своих должностных обязанностей должны производить запись (копирование) информации, осуществляется Информационно-издательским Управлением на основании заявки руководителя структурного подразделения;
- организация обособленной установки серверного и коммуникационного оборудования в отдельных, специально выделенных помещениях (серверных), которые должны находиться под замком и вход в которые должен быть максимально ограничен;
- регистрация печатных копий и электронных носителей документов, содержащих конфиденциальную информацию;
- исключение несанкционированного доступа к информационным массивам, содержащим конфиденциальную информацию;
- недопущение передачи конфиденциальных сведений по незащищенным каналам связи.

9. ЗАЩИТА КОНФИДЕНЦИАЛЬНОЙ РЕЧЕВОЙ ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

9.1. Сохранность речевой информации от утечки по техническим каналам достигается выполнением следующих основных мероприятий и требований:

- документальное определение перечня помещений (защищаемые помещения), специально предназначенных для проведения конфиденциальных мероприятий (совещаний, обсуждений, конференций, переговоров и т.п.);
- обеспечение режимных мер доступа в защищаемые помещения, к техническим средствам передачи и обработки информации, к кабельным коммуникациям;
- ведение переговоров, совещаний по вопросам, содержащим коммерческую тайну, в защищаемых помещениях (по защищенным каналам связи);
- проведение периодического контроля состояния защиты информации в защищаемых помещениях;
- проведение, по решению руководства Статкомитета СНГ, специальных проверок и специальных исследований помещений, технических средств, применяемых для обработки информации, содержащей конфиденциальные сведения. Средства аудио- и видеозаписи, аппаратура звукоусиления, используемые для обработки конфиденциальной информации, должны проходить специальную проверку и специальные исследования в обязательном порядке;
- запрещение использования во время проведения конфиденциальных мероприятий в защищаемых помещениях радиотелефонов (радиостанций), телефонов сотовой связи, мобильных компьютеров (ноутбуки и КПК);
- применение сертифицированных средств защиты информации;

9.2. Организация работ по защите речевой информации от утечки по техническим каналам осуществляется специалистами отдела информационных технологий.

9.3. Ответственность за соблюдение требований по защите информации возлагается на руководителей структурных подразделений, эксплуатирующих защищаемые помещения.

9.4. Контроль состояния защиты речевой информации в защищаемых помещениях от утечки по техническим каналам организуется и проводится ИТ-отделом.

10. ТРЕБОВАНИЯ ПО ОБОРУДОВАНИЮ ПОМЕЩЕНИЙ И РАБОЧИХ МЕСТ

10.1. Входные двери (окна) помещений, в которых производится обработка и хранение документов, содержащих конфиденциальную информацию, должны иметь замки (запоры), гарантирующие надежное их закрытие, и быть оборудованы устройствами для опечатывания.

10.2. Порядок использования ключей (механических, электронных) должен исключать несанкционированный доступ в эти помещения посторонних лиц.

10.3. Для хранения документов, содержащих конфиденциальную информацию, сотрудники обеспечиваются сейфами (запирающимися шкафами), а также необходимым количеством папок и иной оргтехники.

10.4. Порядок опечатывания сейфов (шкафов), входных дверей определяется руководителем подразделения. Обязательному закрытию и опечатыванию подлежат сейфы (запирающиеся шкафы) с конфиденциальными документами и машинными носителями, размещающиеся в общих коридорах.

10.5. Установка и замена оборудования, мебели, ремонт защищаемых помещений должны производиться по согласованию с председателем Статкомитета СНГ либо его заместителем.

11. ПОРЯДОК ПРЕДОСТАВЛЕНИЯ И ПЕРЕДАЧИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ СТОРОННИМ ОРГАНИЗАЦИЯМ

11.1. Предоставление информации о деятельности Статкомитета СНГ органам государственной власти, иным государственным органам, органам местного самоуправления осуществляется в порядке, установленном законодательством на основании мотивированного запроса, подписанного уполномоченным должностным лицом.

11.2. Передача информации контрагентам (юридическим или физическим лицам) Статкомитета СНГ осуществляется на основании договора в объеме и на условиях, которые предусмотрены договором.

11.2.1. Соглашение о неразглашении информации, определяющее условия конфиденциальности, срок их действия и порядок передачи конфиденциальной информации, заключается как неотъемлемое приложение к договору на выполнение работ (оказание услуг, поставки и т.п.). Допускается условия обеспечения конфиденциальности оформлять отдельным разделом договора.

11.2.2. Если при подготовке к заключению договора необходимо ознакомление контрагента с конфиденциальными сведениями Статкомитета СНГ, соглашение о неразглашении информации заключается до передачи этих конфиденциальных сведений и заключения основного договора, с последующим уточнением при необходимости условий конфиденциальности в соглашении о неразглашении информации, заключаемом одновременно с основным договором. В этом случае соглашение о неразглашении информации (соглашение о конфиденциальности) заключается и оформляется отдельным документом в соответствии с порядком, установленным в Статкомитете СНГ для заключения договоров.

11.2.3. Если при заключении Статкомитетом СНГ договора предполагается, что в ходе выполнения работ будут разрабатываться конфиденциальные документы для их последующей передачи Статкомитету СНГ или другим юридическим (физическим) лицам, то в соглашении о неразглашении информации может предусматриваться передача контрагенту Перечня конфиденциальных сведений в объеме, минимально необходимом для надлежащего исполнения этого договора.

11.2.4. Право подписи от имени Статкомитета СНГ Соглашения о неразглашении информации предоставляется Председатель Статкомитета СНГ - на основании Положения, а также другим лицам - на основании доверенности, оформленной установленным порядком.

11.3. Предоставление конфиденциальной информации сторонним организациям, не являющимся контрагентами Статкомитета СНГ, осуществляется на основании мотивированного запроса по письменному разрешению председателя Статкомитета СНГ.

Предварительно руководитель структурного подразделения, которому поручено исполнение запроса, совместно с Управлением делами в срок, не превышающий трех рабочих дней, проводит оценку обоснованности запроса, соответствия тематики и объема информации целям и задачам, которые должны решаться в результате ее получения.

11.4. Передача конфиденциальной информации должна осуществляться, как правило, на бумажных носителях, если их передача на иных носителях не предусмотрена действующим законодательством либо условиями заключенных договоров. В случае, когда подлежащие передаче документы содержат конфиденциальную информацию, обязательно проставление на них соответствующего ограничительного грифа.

11.4.1. В случае обоснованной необходимости передача конфиденциальных сведений на машинном носителе осуществляется с сопроводительным письмом, в соответствии с порядком, определенным в Статкомитете СНГ. В сопроводительном письме указываются перечень и ограничительный гриф отдельных файлов (информационных массивов), записанных на данном носителе. Гриф, проставляемый на самом машинном носителе,

должен быть не ниже высшего ограничительного грифа информации, на нем записанной.

11.4.2. Передача конфиденциальной информации сторонним организациям на машинных носителях, в том числе запись информации на машинные носители принимающей стороны, без разрешения председателя Статкомитета СНГ или уполномоченных им лиц запрещается.

12. ПОРЯДОК ДОСТУПА К ИНФОРМАЦИОННЫМ РЕСУРСАМ СТАТКОМИТЕТА СНГ РАБОТНИКОВ СТОРОННИХ ОРГАНИЗАЦИЙ

12.1. Доступ командированных в Статкомитет СНГ работников сторонних организаций к конфиденциальной информации и документам осуществляется решением председателя Статкомитета СНГ в объеме, необходимом исключительно для выполнения задач командировки.

12.2. Доступ к ресурсам электронных информационных систем осуществляется на основании заявки, оформляемой порядком и по форме, установленным для сотрудников Статкомитета СНГ. Заявка подписывается Председателем Статкомитета СНГ или его заместителем, руководителем соответствующего структурного подразделения, в которое прибыл командированный работник, и согласовывается с Информационно-издательским управлением.

12.3. Непосредственный доступ к ресурсам электронных информационных систем осуществляет ИТ-отдел.

12.4. В общем порядке доступ представителей сторонних организаций, а также физических лиц, оказывающих услуги (выполняющих работы) для Статкомитета СНГ, к электронным источникам информации запрещен.

12.4.1. К совершению отдельных операций с использованием электронных информационных систем Статкомитета СНГ представители сторонних организаций допускаются на основании заключенных договоров или с письменного разрешения Председателя Статкомитета СНГ или лица, его замещающего.

12.4.2. На представителей сторонних организаций, допускаемых к совершению отдельных операций с использованием электронных информационных систем Статкомитета СНГ, оформляется заявка в соответствии с порядком и по форме, которые установлены для сотрудников Статкомитета СНГ.

12.4.3. На каждого представителя контрагента Информационно-издательским управлением оформляется отдельная учетная запись в порядке, установленном соответствующими регламентами.

Примечание – Данный порядок доступа к электронным информационным системам Статкомитета СНГ распространяется и на представителей органов государственной власти, иных государственных органов, выполняющих свои функции в соответствии с действующим законодательством.

12.5. Контроль соблюдения представителями сторонних организаций установленного в Статкомитете СНГ режима конфиденциальности при использовании электронных информационных систем возлагается на руководителей структурных подразделений, к которым прибыли представители.

13. ОПУБЛИКОВАНИЕ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ В СРЕДСТВАХ МАССОВОЙ ИНФОРМАЦИИ

13.1. Запрещается публикация материалов, содержащих конфиденциальные сведения, в средствах массовой информации, включая Интернет и другие публичные компьютерные сети, а также использование их в публичных выступлениях до снятия в

установленном порядке существующих ограничений.

13.2. Возможность открытого оглашения (публикации) конфиденциальных сведений, обладателем которых является Статкомитет СНГ, определяется решением Председателя Статкомитета СНГ.

Открытое оглашение (публикация) конфиденциальных сведений, в отношении которых Статкомитет СНГ не является обладателем (собственником), может осуществляться при наличии письменного согласия обладателя (собственника) этой информации на ее открытое оглашение (публикацию), а также в иных случаях, предусмотренных действующим законодательством.

13.3. В случае принятия такого решения и открытого оглашения (публикации) сведений:

- сведения утрачивают статус конфиденциальности, в отношении этих сведений утрачивает действие режим конфиденциальности, установленный в Статкомитете СНГ Положением и другими разработанными на его основе нормативными документами;
- на документах, содержащих эти сведения, ограничительный гриф «К» снимается;
- в отношении этих сведений утрачивается действие обязательства и условия конфиденциальности в действующих договорах (соглашениях, контрактах), заключенных ранее.

13.5. При публикации в средствах массовой информации, включая Интернет и другие публичные компьютерные сети, статей, касающихся деятельности Статкомитета СНГ, сотрудники - авторы статей обязаны соотносить используемый в публикациях материал с действующим в Статкомитете СНГ Перечнем конфиденциальных сведений.

13.5.1. Перед публикацией статьи должны обязательно согласовываться (рецензироваться) с ответственным лицом Статкомитета СНГ с указанием в рецензиях фразы: "Использованные в статье материалы конфиденциальных сведений не содержат".

13.6. Сотрудники, обнаружившие факт публикации в средствах массовой информации, включая Интернет, а также использования в публичных выступлениях конфиденциальных сведений, в отношении которых в Статкомитете СНГ установлен режим конфиденциальности, обязаны сообщить об этом своему непосредственному руководителю.

14. ПОРЯДОК ОБРАЩЕНИЯ С КОНФИДЕНЦИАЛЬНЫМИ СВЕДЕНИЯМИ

14.1. К сведениям, которые Статкомитета СНГ, имеющим конфиденциальный характер, относятся:

- а) информация служебного характера:
 - статистические и отчетные документы, форма и содержание которых установлены нормативными актами органов государственной власти;
 - платежные документы;
 - сведения об исчислении и уплате налогов и обязательных платежей, о численности и составе работающих, их заработной плате и др.;
- б) служебные сведения, доступ к которым ограничен органами государственной власти;
- в) конфиденциальные сведения, защищаемые государством в иных режимах:
 - сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность (персональные данные);
 - сведения, связанные с профессиональной деятельностью, доступ к которым ограничен;
 - сведения, составляющие тайну следствия и судопроизводства;
 - сведения, защищаемые нормами патентного, авторско-правового и иного

специального законодательства.

14.2. Отнесение сведений к этой категории осуществляется на основании отдельной графы Перечня.

Документальным материалам, которые носят конфиденциальный характер, но не содержат информации, составляющей коммерческую тайну Общества, присваивается ограничительный гриф "Конфиденциально" ("К").

14.3. На документах, указанных в пп. "а" п. 14.1, и документах, конфиденциальность которых определена законом и порядок учета, хранения и обращения с которыми определяется специальными нормами законодательства, ограничительный гриф "К" не проставляется.

14.4. Поступающие из государственных структур документы, содержащие служебную тайну, с проставленным на них ограничительным грифом "Для служебного пользования" (ДСП), являются конфиденциальными по своему статусу, и на них распространяется режим защиты, установленный настоящим Положением для конфиденциальных материалов.

14.5. Документооборот материалов с ограничительным грифом "Конфиденциально", а равно и с пометкой "Для служебного пользования", осуществляется в системе общего делопроизводства с соблюдением требований нормативных документов Статкомитета СНГ и Положения.

14.6. Обработка и передача конфиденциальной информации с использованием СВТ осуществляется с соблюдением требований, изложенных в Положении.

15. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

15.1 Разглашение конфиденциальных сведений Статкомитета СНГ, или утрата документов, содержащих таковую, относится к числу грубых нарушений трудовых обязанностей.

15.2. За разглашение конфиденциальных сведений Статкомитета СНГ и его контрагентов, утрату документов, содержащих такие сведения, а также за иные нарушение установленного в Статкомитете СНГ порядка учета, хранения, обращения с конфиденциальными документами и информацией виновные несут дисциплинарную ответственность, применяемую к подобного рода нарушениям в соответствии с действующими в Статкомитете СНГ локальными нормативными актами и действующим законодательством ответственность.

16. ПРОВЕДЕНИЕ СЛУЖЕБНОГО РАССЛЕДОВАНИЯ ПО ФАКТАМ РАЗГЛАШЕНИЯ (УТРАТЫ) КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ

16.1. По фактам разглашения (утраты) конфиденциальных сведений проводится служебное расследование.

Служебное расследование может также назначаться по фактам грубого нарушения установленных нормативными документами правил обращения с конфиденциальной информацией.

Для проведения служебного расследования приказом председателя Статкомитета СНГ или его заместителя назначается комиссия в составе не менее трех человек.

Руководитель структурного подразделения, проверяемого по фактам разглашения (утраты) конфиденциальных сведений принимает активное участие в обеспечении работы комиссии.

16.2. Комиссия, проводящая служебное расследование:

- выясняет обстоятельства, причины разглашения сведений или утраты документов, а также способствовавшие этому условия;
- устанавливает лиц, виновных в разглашении сведений или утрате документов;
- принимает меры к розыску утраченного документа или предотвращению негативных последствий разглашения сведений.

16.3. Члены комиссии, проводящие служебное расследование, имеют право:

- производить осмотр помещений Статкомитета СНГ (сейфов, столов, шкафов, и т.д.);
- проверять конфиденциальную документацию, журналы учета конфиденциальных документов;
- опрашивать сотрудников Статкомитета СНГ, виновных в утрате (разглашении), а также других сотрудников Статкомитета СНГ, могущих оказать содействие в установлении обстоятельств происшедшего и получать от них письменные объяснения;
- привлекать сотрудников других структурных подразделений, не заинтересованных в исходе дела, для проведения отдельных действий служебного расследования по согласованию с их руководителями.

16.4. Служебное расследование проводится в минимально короткий срок, но не более 10 рабочих дней со дня назначения комиссии. В случаях, когда в течение данного срока утраченные документы не обнаружены, поиск их может быть прекращен.

16.5. По результатам расследования составляется заключение, в котором отражаются следующие вопросы:

- основания для проведения расследования;
- кто и в какие сроки проводил расследование;
- перечень и результаты осуществленных мероприятий;
- виновные лица;
- выявленные причины и условия, способствовавшие разглашению (утрате);
- мнение о наличии в действиях виновного лица признаков административного правонарушения либо уголовно наказуемого деяния;
- возможные негативные последствия происшедшего для интересов Статкомитета СНГ и предложения по их устранению.

16.6. Заключение по результатам служебного расследования докладывается председателю Статкомитета СНГ для принятия решения о привлечении виновного к дисциплинарной ответственности либо о передаче материалов в правоохранительные или судебные органы, а также о мерах по устранению причин и возможных негативных последствий происшедшего либо об отклонении материалов расследования.

17. ОРГАНИЗАЦИЯ КОНТРОЛЯ СОХРАННОСТИ КОНФИДЕНЦИАЛЬНЫХ СВЕДЕНИЙ

17.1. Общая организация контроля состояния установленного в Статкомитета СНГ режима конфиденциальности возлагается на председателя Статкомитета СНГ.

17.2. Контроль выполнения правил обращения с информацией, содержащей конфиденциальные сведения, требований настоящего Положения осуществляют заместители Председателя Статкомитета СНГ по направлениям деятельности и руководители структурных подразделений Статкомитета СНГ.

17.3. Контроль обеспечения сохранности конфиденциальных сведений может осуществляться в форме:

- повседневного контроля правил соблюдения режимных требований (без составления акта);

- ежегодных проверок документированной информации;
- плановой проверки в конкретном структурном подразделении или на конкретном участке работы (на рабочем месте);
- внеплановой проверки по конкретному вопросу по указанию председателя Статкомитета СНГ или его заместителя.

17.4. Результаты проверок оформляются актами, в которых отражаются основания проверки, кем и когда она проводилась, оценка состояния работы по обеспечению конфиденциальности, необходимые предложения и рекомендации по устранению недостатков и совершенствованию ее защиты.

Акт проверки докладывается Председателю Статкомитета СНГ для принятия решения.

18. ПОРЯДОК ВНЕСЕНИЯ ИЗМЕНЕНИЙ И ДОПОЛНЕНИЙ

18.1. Положение утверждается, изменяется, дополняется и вводится в действие приказом Председателя Статкомитета СНГ.

18.2. Сбор и обобщение предложений по внесению изменений и дополнений в действующий документ осуществляется Управлением делами, которое организует работу по рассмотрению поданных предложений для определения целесообразности внесения соответствующих корректировок.

18.3. Рассмотренные предложения с заключением об их целесообразности представляются председателю Статкомитета СНГ для принятия решения. При принятии положительного решения определяются ответственные лица за подготовку проекта приказа председателя Статкомитета СНГ о внесении изменений в действующий документ.