

ПРИКАЗ

«21» *апреля* 2023 г.

№ *38-0*

г. Вологда

**О защите информации на автоматизированных рабочих местах,
предназначенных для обработки служебной информации ограниченного
распространения**

В целях реализации постановления Губернатора области от 28 июня 2012 года № 358 «О передаче обеспечивающих функций», обеспечения защиты информации на автоматизированных рабочих местах, предназначенных для обработки служебной информации ограниченного распространения, руководствуясь пунктом 3.1.4 Положения о Департаменте цифрового развития области, утвержденного постановлением Правительства области от 13 декабря 2021 года № 1395

ПРИКАЗЫВАЮ:

1. Утвердить:

1.1 Методические рекомендации по защите информации на автоматизированных рабочих местах, предназначенных для обработки служебной информации ограниченного распространения в органах исполнительной государственной власти области, государственных учреждениях области (приложение 1);

1.2 Инструкцию системного администратора автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения (приложение 2);

1.3 Положение о Реестре автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения в органах исполнительной государственной власти области, государственных учреждениях области (приложение 3).

2. Рекомендовать органам исполнительной государственной власти области,

государственным учреждениям области, в случае передачи обеспечивающих функций в сфере информационных технологий подведомственному учреждению Департамента цифрового развития Вологодской области в соответствии с постановлением Губернатора области, организовать эксплуатацию автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения в соответствии с Методическими рекомендациями, указанными в п. 1 настоящего приказа.

3. Директору бюджетного учреждения в сфере информационных технологий Вологодской области «Центр информационных технологий» Н.А. Пучкову:

3.1 обеспечить исполнение Инструкции системного администратора автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения в органах исполнительной государственной власти области, государственных учреждениях области;

3.2 в месячный срок со дня вступления в силу настоящего приказа обеспечить формирование Реестра автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения в органах исполнительной государственной власти области, государственных учреждениях области, а также назначить ответственных лиц за ведение и своевременную актуализацию указанного Реестра.

4. Контроль за исполнением настоящего приказа оставляю за собой.

5. Настоящий приказ вступает в силу со дня его официального опубликования.

Начальник Департамента



И.В. Просвирякова

УТВЕРЖДЕНЫ

приказом Департамента цифрового
развития области

от «21» сентября 2023 г. № 38 - 0
(приложение 1)

**Методические рекомендации
по защите информации на автоматизированных рабочих местах,
предназначенных для обработки служебной информации ограниченного
распространения в органах исполнительной государственной власти
области, государственных учреждениях области
(далее – Методические рекомендации)**

Настоящие Методические рекомендации разработаны в целях защиты информации на автоматизированных рабочих местах, предназначенных для обработки служебной информации ограниченного распространения и определяют перечень организационных мероприятий, которые рекомендуется реализовать в органах исполнительной государственной власти и государственных учреждениях Вологодской области, в случае передачи обеспечивающих функций в сфере информационных технологий подведомственному учреждению Департамента цифрового развития Вологодской области в соответствии с постановлением Губернатора области.

В целях защиты информации на автоматизированных рабочих местах, предназначенных для обработки служебной информации ограниченного распространения органам исполнительной государственной власти (далее - орган) и государственным учреждениям (далее - учреждение) Вологодской области рекомендуется:

1. Назначить ответственное лицо из числа сотрудников органа/учреждения за эксплуатацию автоматизированного рабочего места, предназначенного для обработки служебной информации ограниченного распространения (далее – Ответственное лицо).

2. Разработать и утвердить по согласованию с БУ ВО «ЦИТ» Технический паспорт объекта информатизации. Типовая форма Технического паспорта приведена в Приложении 1 к Методическим рекомендациям.

3. Утвердить (по согласованию с БУ ВО «ЦИТ») приказом органа/учреждения:

а). Инструкцию лица, ответственного за эксплуатацию автоматизированного рабочего места, предназначенного для обработки служебной информации ограниченного распространения. Типовая форма Инструкции приведена в Приложении 2 к Методическим рекомендациям.

б). Регламент доступа к автоматизированным рабочим местам, предназначенным для обработки служебной информации ограниченного распространения. Типовая форма Регламента приведена в Приложении 3 к Методическим рекомендациям.

в). Инструкцию пользователя автоматизированного рабочего места, предназначенного для обработки служебной информации ограниченного

распространения. Типовая форма Инструкции приведена в Приложении 4 к Методическим рекомендациям.

г). Требования к системе защиты информации автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения. Типовая форма Требований приведена в Приложении 5 к Методическим рекомендациям.

д). Матрицу доступа к защищаемым информационным ресурсам автоматизированного рабочего места, предназначенного для обработки служебной информации ограниченного распространения. Типовая форма Матрицы доступа приведена в Приложении 6 к Методическим рекомендациям.

е). Состав комиссии по защите информации на автоматизированных рабочих местах, предназначенных для обработки служебной информации ограниченного распространения. В обязательном порядке в состав комиссии включаются руководитель и (или) заместитель руководителя органа/учреждения, Ответственное лицо, представитель БУ ВО «ЦИТ» (по согласованию) и иные сотрудники органа/учреждения.

ж). Форму Журнала учета машинных носителей информации, предназначенных для хранения и обработки служебной информации ограниченного распространения. Типовая форма Журнала приведена в Приложении 8 к Методическим рекомендациям.

з). Форму Журнала регистрации работ на автоматизированном рабочем месте, предназначенном для обработки служебной информации ограниченного распространения. Типовая форма Журнала приведена в Приложении 9 к Методическим рекомендациям.

4. Комиссии по защите информации, указанной в п. 3 настоящих Методических рекомендаций провести классификацию автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения. Результат работы комиссии оформляется в виде Акта классификации, типовая форма которого приведена в Приложении 7 к Методическим рекомендациям.

5. По итогам реализации организационных мероприятий по защите информации на автоматизированных рабочих местах, предназначенных для обработки служебной информации ограниченного распространения, комиссии по защите информации, указанной в п. 3 настоящих Методических рекомендаций необходимо провести оценку эффективности реализованных мер по защите информации. Результат работы комиссии оформляется в виде Протокола, типовая форма которого приведена в Приложении 10 к Методическим рекомендациям.

6. Ознакомить сотрудников органа/учреждения с приказом указанным в п. 3 настоящих Методических рекомендаций.

7. Эксплуатация автоматизированного рабочего места, предназначенного для обработки служебной информации ограниченного распространения без Протокола оценки эффективности реализованных мер по защите информации и ознакомления сотрудников с организационной – распорядительной документацией, указанной в настоящих Методических рекомендациях, не допускается.

Приложение 1
к Методическим рекомендациям по защите
информации на автоматизированных
рабочих местах, предназначенных для
обработки служебной информации
ограниченного распространения в органах
исполнительной государственной власти
области, государственных учреждениях
области

ТИПОВАЯ ФОРМА

СОГЛАСОВАНО

Директор БУ ВО «Центр
информационных технологий»

УТВЕРЖДАЮ

Руководитель органа исполнительной
государственной власти/государственного
учреждений области

_____ И.О. Фамилия

_____ И.О. Фамилия

«___» _____ 202__ г.

«___» _____ 202__ г.

ТЕХНИЧЕСКИЙ ПАСПОРТ
объекта информатизации

Автоматизированное рабочее место - АРМ ДСП № __, предназначенное для
обработки служебной информации ограниченного распространения

г. Вологда

202__ год

1. Общие сведения об объекте информатизации

Наименование объекта информатизации: Автоматизированное рабочее
место - АРМ ДСП № __, предназначенное для обработки служебной информации
ограниченного распространения.

Оператор объекта информатизации: Наименование органа исполнительной
государственной власти/государственного учреждений Вологодской области.

Адрес объекта, где размещен объект информатизации: Россия, г. Вологда,
ул. _____, д. __, к. __ на __ этаже здания.

2. Состав объекта информатизации

2.1. Перечень основных технических средств и систем (ОТСС), входящих в
состав объекта информатизации:

Таблица № 1

№ п/п	Тип технических средств	Марка, модель	Серийный/ инвентарный номер	Место размещения
1	2	3	4	5
1	АРМ ДСП №			
1.1	Системный блок (ОТСС)	_____	Инв. № _____	Россия, г. Вологда, ул. _____, д. _____, к. ____
1.2	Монитор (ОТСС)	_____	Инв. № _____	
1.3	Принтер (ВТСС)	_____	Инв. № _____	

2.2. Структура, топология и размещение ОТСС на объекте:

Схема размещения ОТСС на объекте приведена в Приложении № 1 к настоящему Техническому паспорту.

2.3. Перечень средств защиты информации, применяемых на объекте информатизации:

Таблица № 2

№ п/п	Наименование программного средства	Сведения о лицензии (номер лицензии, тип)	Место установки
1	2	3	5
1	Антивирусное ПО		АРМ ДСП № __
2	Операционная система	Лицензионное свидетельство права на использование программного обеспечения по программе лицензирования	АРМ ДСП № __

2.4. Сведения об используемом на объекте информатизации программном обеспечении:

Таблица № 3

№ п/п	Наименование программного средства	Сведения о лицензии (номер лицензии, тип)	Место установки
1	2	3	4
1	Операционная система	Лицензионное свидетельство права на использование ПО по программе лицензирования	АРМ ДСП № __
2		Лицензионное свидетельство права на использование ПО по программе лицензирования	АРМ ДСП № __

3. Результаты периодического контроля

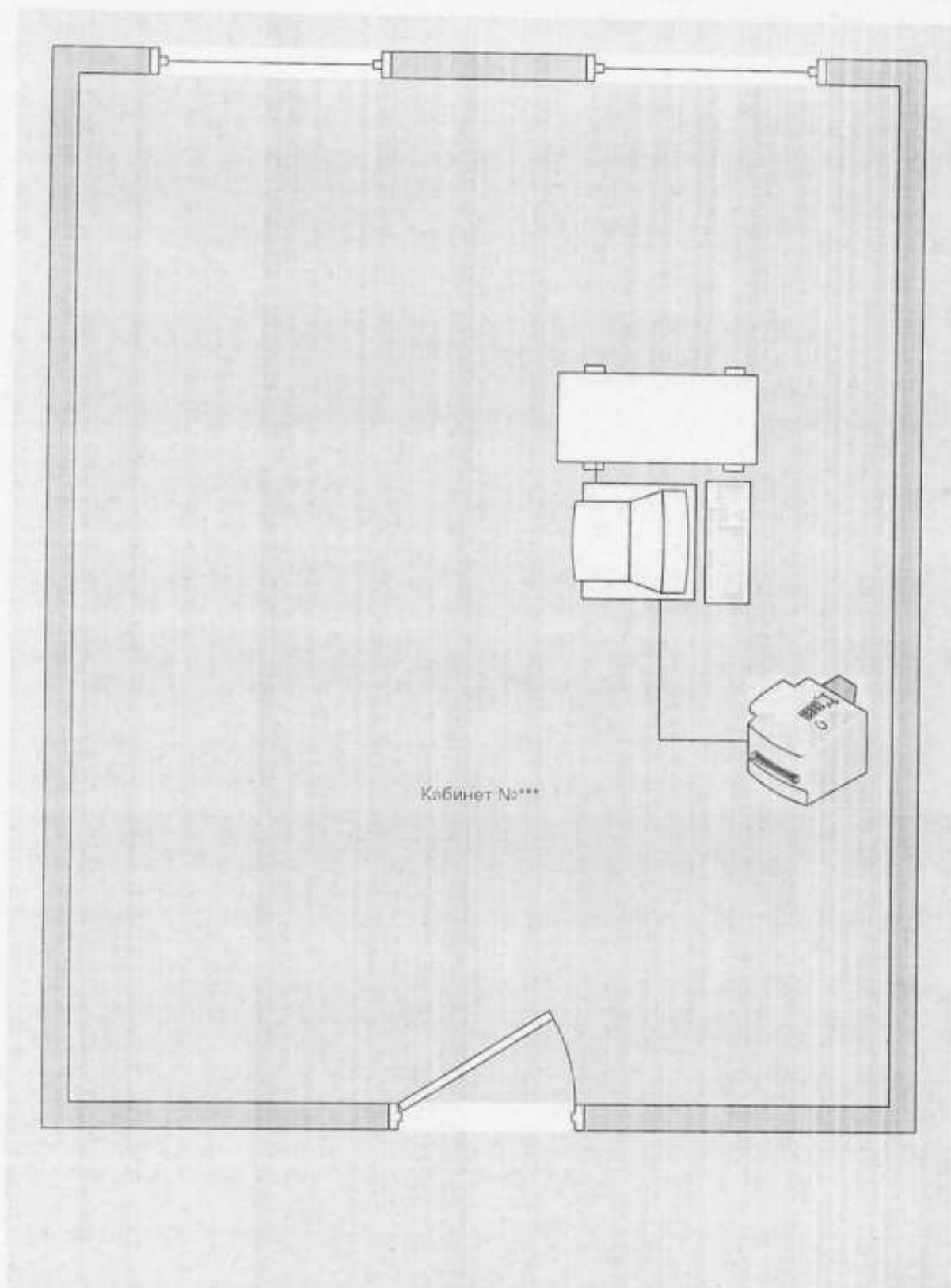
Дата проведения	Наименование организации, проводившей проверку	Результаты проверки, номер отчётного документа

4. Лист регистрации изменений

№ п/п	Наименование документа, номера изменённых листов	Дата изменений	ФИО ответственного лица, подпись
1			
2			

Приложение № 1
к Техническому паспорту
объекта информатизации

Схема размещения и расположения ОТСС на объекте



Приложение 2
к Методическим рекомендациям по защите
информации на автоматизированных
рабочих местах, предназначенных для
обработки служебной информации
ограниченного распространения в органах
исполнительной государственной власти
области, государственных учреждениях
области

ТИПОВАЯ ФОРМА

ИНСТРУКЦИЯ

лица, ответственного за эксплуатацию автоматизированного рабочего места,
предназначенного для обработки служебной информации ограниченного
распространения

1. Общие положения

1.1. Настоящая инструкция лица, ответственного за эксплуатацию автоматизированного рабочего места, предназначенного для обработки служебной информации ограниченного распространения (далее – АРМ ДСП), определяет обязанности, полномочия и ответственность лица, ответственного за эксплуатацию АРМ ДСП (далее – ответственный за эксплуатацию АРМ ДСП).

1.2. Ответственный за эксплуатацию АРМ ДСП назначается приказом руководителя органа исполнительной государственной власти, государственного учреждения Вологодской области. Ответственным за АРМ ДСП рекомендуется назначать сотрудника, в должностные обязанности которого входит учет (регистрация), исполнение и хранение документов, содержащих служебную информацию ограниченного распространения.

2. Обязанности ответственного за эксплуатацию АРМ ДСП

Ответственный за эксплуатацию АРМ ДСП обязан:

2.1. Организовывать доступ пользователей к работе на АРМ ДСП.

2.2. Вести Журнал учета машинных носителей информации, предназначенных для хранения и обработки служебной информации ограниченного распространения, фиксируя в нем носители информации, встроенные в АРМ ДСП и используемые отчуждаемые машинные носители (CD и DVD диски, другие съемные носители информации).

2.3. Организовывать ведение Журнала регистрации работы на автоматизированном рабочем месте, предназначенном для обработки служебной информации ограниченного распространения, в котором фиксируются время работы пользователей на АРМ ДСП и цель использования АРМ ДСП.

- 2.4. Не допускать посторонних лиц к работе на АРМ ДСП.
- 2.5. Взаимодействовать с БУ ВО «ЦИТ» по вопросам сопровождения, администрирования и технической поддержки АРМ ДСП.
- 2.6. При первичном доступе пользователей к автоматизированной обработке служебной информации ограниченного распространения на АРМ ДСП: проводить инструктаж по использованию АРМ ДСП; доводить (под подпись) до пользователей, обрабатывающих служебную информацию ограниченного распространения на АРМ ДСП, требования организационно-распорядительных документов, регламентирующих обработку служебной информации ограниченного распространения;
- 2.7. При получении от пользователя информации о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации немедленно сообщать об этом системному администратору АРМ ДСП для принятия мер по блокированию учетной записи пользователя.
- 2.8. При получении от пользователя информации о фактах вирусного заражения АРМ ДСП сообщать о факте заражения системному администратору АРМ ДСП для организации внеочередного полного антивирусного сканирования АРМ ДСП (в том числе и машинных носителей информации, которые подключались к заражённому АРМ ДСП).
- 2.9. Организовывать периодический (не реже, чем один раз в месяц) запуск сканера антивирусного программного обеспечения.
- 2.10. В случае прекращения полномочий (увольнение) пользователя незамедлительно через ИС Помощник <https://help.gov35.ru> направлять заявку в БУ ВО «ЦИТ» на удаление учетной записи пользователя АРМ ДСП.

3. Ответственность

Ответственный за эксплуатацию АРМ ДСП несет ответственность, установленную законодательством Российской Федерации за сохранность и неразглашение служебной информации ограниченного распространения и за соблюдение требований настоящей Инструкции.

Приложение 3

к Методическим рекомендациям по защите информации на автоматизированных рабочих местах, предназначенных для обработки служебной информации ограниченного распространения в органах исполнительной государственной власти области, государственных учреждениях области

ТИПОВАЯ ФОРМА

РЕГЛАМЕНТ

доступа к автоматизированным рабочим местам, предназначенным для обработки служебной информации ограниченного распространения

1. Общие положения

1.1. В настоящем Регламенте определяется порядок организации работ по разграничению доступа пользователей к средствам защиты и информационным ресурсам, содержащим служебную информацию ограниченного распространения, обрабатываемую на автоматизированных рабочих местах (далее – АРМ ДСП) в органах исполнительной государственной власти и государственных учреждениях Вологодской области.

1.2. Автоматизированная обработка служебной информации ограниченного распространения допускается только на базе автономных АРМ ДСП или в локальных вычислительных сетях (далее – ЛВС), расположенных в пределах контролируемой зоны, если ЛВС не имеет подключения к другим автоматизированным информационным системам.

1.3. Регламент определяет:

порядок выполнения процедур по предоставлению и прекращению доступа к информационным ресурсам на АРМ ДСП;

порядок обеспечения процессов идентификации и аутентификации пользователей защищаемых информационных ресурсов на АРМ ДСП;

порядок работы с парольной документацией, в том числе генерации, смены и прекращения действия паролей, меры обеспечения безопасности при использовании паролей на АРМ ДСП;

требования к средствам защиты и обслуживанию технических средств и систем АРМ ДСП.

1.4. Настоящий Регламент устанавливает порядок работы с защищаемой информацией в целях:

предотвращения несанкционированного доступа к служебной информации ограниченного распространения;

предотвращения несанкционированного уничтожения, искажения, копирования, блокирования служебной информации ограниченного распространения.

1.5. Основными видами угроз безопасности служебной информации

ограниченного распространения (модификации, блокированию, уничтожению или несанкционированному копированию) при ее обработке на АРМ ДСП, являются:

- противоправные действия третьих лиц;
- противоправные действия пользователей;
- ошибочные действия пользователей, в том числе нарушения правил эксплуатации ЭВМ и сетевого оборудования;
- отказы и сбои технических средств.

1.6. Системными администраторами, ответственными за сопровождение, администрирование и техническую поддержку АРМ ДСП, являются работники бюджетного учреждения в сфере информационных технологий Вологодской области «Центр информационных технологий» (далее – БУ ВО «ЦИТ»).

1.7. Пользователи АРМ ДСП и ответственный за эксплуатацию АРМ ДСП несут персональную ответственность за сохранность, неразглашение служебной информации ограниченного распространения и за соблюдение требований Инструкции о порядке обращения со служебной информацией ограниченного распространения, утвержденной в органе исполнительной государственной власти, государственном учреждении Вологодской области, Инструкции пользователя АРМ ДСП и настоящего Регламента.

1.8. За разглашение служебной информации ограниченного распространения, нарушение порядка обращения с документами или материальными носителями, содержащими такую информацию, пользователь АРМ ДСП может быть привлечен к дисциплинарной или иной предусмотренной законодательством Российской Федерации ответственности.

2. Предоставление пользователям доступа к АРМ ДСП

2.1. Технические мероприятия по вводу в эксплуатацию АРМ ДСП, его оснащению и настройке режима работы осуществляет системный администратор АРМ ДСП.

2.2. Доступ пользователей к работе на АРМ ДСП организует ответственный за эксплуатацию АРМ ДСП, который в том числе отвечает за соблюдение требований по защите информации ограниченного распространения при ее обработке на АРМ ДСП в органе исполнительной государственной власти, государственном учреждении Вологодской области.

2.3. Заявка на создание учетной записи пользователя АРМ ДСП и предоставление ему доступа к защищаемым ресурсам АРМ ДСП направляется в БУ ВО «ЦИТ» пользователем АРМ ДСП через ИС Помощник <https://help.gov35.ru>.

2.4. При первичном доступе к автоматизированной обработке служебной информации ограниченного распространения на АРМ ДСП пользователь:

проходит у ответственного за эксплуатацию АРМ ДСП инструктаж по использованию АРМ ДСП;

знакомится с требованиями организационно-распорядительных документов, регламентирующих обработку служебной информации ограниченного распространения;

2.5. Все действия пользователей АРМ ДСП в отношении АРМ ДСП подлежат фиксации в Журнале регистрации работы на автоматизированном

рабочем месте, предназначенном для обработки служебной информации ограниченного распространения.

3. Общие требования к паролям пользователей АРМ ДСП

3.1. В АРМ ДСП используется однофакторная аутентификация пользователей. Допуск пользователей к обработке служебной информации ограниченного распространения на АРМ ДСП осуществляется на основании идентификатора и аутентификатора. В качестве аутентификатора пользователя используется личный пароль. Аутентификация пользователя в АРМ ДСП выполняется при входе в систему.

3.2. При первичном доступе пользователя системный администратор АРМ ДСП формирует идентификатор пользователя (имя пользователя для регистрации на АРМ ДСП) и личный пароль пользователя в соответствии с пунктом 3.6., и передает его пользователю АРМ ДСП. Пользователь обязан сменить личный пароль, предоставленный системным администратором АРМ ДСП при первом входе в систему.

3.3. В случае смены личного пароля пользователь самостоятельно меняет его, руководствуясь правилами, указанными в п. 3.6.

3.4. Доведение до пользователей идентификаторов пользователей и личных паролей, осуществляет системный администратор АРМ ДСП.

3.5. Смена личного пароля должна производиться в обязательном порядке в следующих случаях:

- компрометации (подозрении на компрометацию) пароля;

- по инициативе системного администратора АРМ ДСП или ответственного за АРМ ДСП.

3.6. При формировании пароля необходимо руководствоваться следующими требованиями:

- длина пароля должна быть не менее 8-и буквенно-цифровых символов;

- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;

- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

- запрещается использовать ранее использованные пароли.

3.7. При использовании пароля пользователю запрещается:

- записывать свои пароли в очевидных местах (внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.);

- хранить пароли в записанном виде на отдельных листах бумаги;

- сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от несанкционированного доступа на АРМ ДСП;

- вводить личный пароль и другие учетные данные, если клавиатура находится в поле зрения других лиц.

4. Порядок разграничения прав пользователей и ограничения доступа пользователей к АРМ ДСП

4.1. Для каждого пользователя выделяется доступный только ему ресурс АРМ ДСП (папка).

4.2. Технические средства АРМ ДСП должны находиться в условиях, исключающих несанкционированный доступ. Случайный просмотр экрана монитора АРМ ДСП посторонними людьми должен быть исключён.

5. Требования к средствам защиты и обслуживанию технических средств и систем АРМ ДСП

5.1. При обработке служебной информации ограниченного распространения на АРМ ДСП должны быть реализованы требования к защите информации АРМ ДСП, исходя из класса защищенности АРМ ДСП.

5.2. Запрещается подключать к АРМ ДСП сторонние устройства, отсутствующие в Журнале учета машинных носителей информации, предназначенных для хранения и обработки служебной информации ограниченного распространения и не указанные в Техническом паспорте АРМ ДСП.

5.3. В целях организации упорядоченного и избирательного доступа к АРМ ДСП программное обеспечение, установленное на АРМ ДСП, должно обеспечивать выполнение следующих требований:

осуществляться автоматическая блокировка АРМ ДСП при отсутствии активности пользователя более 5 минут, а также по запросу пользователя;

осуществляться автоматическая блокировка АРМ ДСП в случае пяти неуспешных попыток входа в информационную систему;

гостевая учётная запись АРМ ДСП должна быть заблокирована;

реализован доступ пользователя АРМ ДСП к системе только под учётной записью с ограниченными правами. Запрещается работа с системой в привилегированном режиме (авторизация в системе с учётной записью, имеющей права администратора).

5.4. Ремонт АРМ ДСП, содержащих на носителях информации документы со служебной информацией ограниченного распространения, производится в присутствии ответственного за эксплуатацию АРМ ДСП, исключающего несанкционированный доступ к таким документам.

5.5. Запрещается выносить (вывозить) носители, содержащие служебную информацию ограниченного распространения, за пределы контролируемой зоны органа исполнительной государственной власти, государственного учреждения Вологодской области без разрешения руководителя органа исполнительной государственной власти, государственного учреждения Вологодской области.

При необходимости перемещения АРМ ДСП, содержащего на носителях документы со служебной информацией ограниченного распространения, за пределы контролируемой зоны ответственным за эксплуатацию АРМ ДСП принимаются меры, исключающие возможность их хищения в процессе перемещения, а также несанкционированного доступа к таким документам без

нарушения целостности упаковки АРМ ДСП.

5.6. Неисправные носители информации АРМ ДСП подлежат уничтожению с использованием методов гарантированного стирания информации (в том числе физического уничтожения).

5.7. В случае списания технических средств и (или) систем, хранивших информацию ограниченного доступа, носители информации таких средств и (или) систем подлежат уничтожению с использованием методов гарантированного стирания информации.

5.8. Все действия системного администратора АРМ ДСП в отношении АРМ ДСП подлежат фиксации в Журнале регистрации работы на автоматизированном рабочем месте, предназначенном для обработки служебной информации ограниченного распространения.

6. Требования к антивирусному программному обеспечению

6.1. На АРМ ДСП в обязательном порядке должно быть установлено сертифицированное антивирусное программное обеспечение.

6.2. На АРМ ДСП в обязательном порядке должен периодически (не реже, чем один раз в месяц) запускаться сканер антивирусного программного обеспечения. Контроль за этим осуществляет ответственный за эксплуатацию АРМ ДСП.

6.3. В случае если обнаружены признаки заражения АРМ ДСП программами-вирусами:

6.3.1. Пользователь АРМ ДСП обязан:

немедленно прекратить работу АРМ ДСП;

немедленно сообщить ответственному за АРМ ДСП и системному администратору АРМ ДСП о факте заражения.

6.3.2. Системный администратор АРМ ДСП обязан произвести внеочередное полное антивирусное сканирование АРМ ДСП.

Приложение 4
к Методическим рекомендациям по
защите информации на
автоматизированных рабочих местах,
предназначенных для обработки
служебной информации ограниченного
распространения в органах
исполнительной государственной власти
области, государственных учреждениях
области

ТИПОВАЯ ФОРМА

ИНСТРУКЦИЯ **пользователя автоматизированного рабочего места, предназначенного для** **обработки служебной информации ограниченного распространения**

1. Общие положения

1.1. Настоящая инструкция пользователя автоматизированного рабочего места, предназначенного для обработки служебной информации ограниченного распространения (далее – АРМ ДСП), предназначена для лиц, допущенных к автоматизированной обработке служебной информации ограниченного распространения, и регулирует порядок допуска пользователей к работе на АРМ ДСП, а также правила обращения с защищаемой информацией, обрабатываемой на АРМ ДСП.

1.2. Инструкция пользователя АРМ ДСП (далее – Инструкция) устанавливает порядок работы с защищаемой информацией, в целях:

предотвращения несанкционированного доступа к служебной информации ограниченного распространения;

предотвращения несанкционированного уничтожения, искажения, копирования, блокирования служебной информации ограниченного распространения.

1.3. Пользователи АРМ ДСП перед началом работы на АРМ ДСП должны быть ознакомлены с Инструкцией о порядке обращения со служебной информацией ограниченного распространения, утвержденной в органе исполнительной государственной власти, государственном учреждении Вологодской области и настоящей Инструкцией.

1.4. Пользователи АРМ ДСП несут персональную ответственность за сохранность, неразглашение служебной информации ограниченного распространения и за соблюдение требований настоящей Инструкции. За разглашение служебной информации ограниченного распространения, нарушение порядка обращения с документами или материальными носителями, содержащими такую информацию, пользователь АРМ ДСП может быть привлечен к дисциплинарной или иной предусмотренной законодательством

2. Обязанности пользователя АРМ ДСП

Для работы с документами, содержащими служебную информацию ограниченного распространения на АРМ ДСП каждый пользователь должен получить соответствующий доступ к АРМ ДСП.

2.1. Доступ пользователей к работе на АРМ ДСП организует ответственный за эксплуатацию АРМ ДСП в органе исполнительной государственной власти, государственном учреждении Вологодской области (далее – ответственный за эксплуатацию АРМ ДСП).

2.2. При первичном доступе к автоматизированной обработке служебной информации ограниченного распространения на АРМ ДСП, пользователь:

- проходит у ответственного за эксплуатацию АРМ ДСП инструктаж по эксплуатации АРМ ДСП;

- знакомится с требованиями организационно-распорядительных документов, регламентирующих обработку служебной информации ограниченного распространения;

2.3. Пользователь АРМ ДСП обязан:

- не допускать физическое воздействие на технические средства автоматизированной обработки служебной информации ограниченного распространения, в результате которого может быть нарушено их функционирование;

- незамедлительно сообщить ответственному за АРМ ДСП в случае утраты или компрометации личного пароля;

- в процессе работы использовать только установленные системным администратором АРМ ДСП технические средства и программное обеспечение;

- при работе на АРМ ДСП выполнять только служебные задания;

- работать на АРМ ДСП с фиксацией в Журнале регистрации работы на автоматизированном рабочем месте, предназначенном для обработки служебной информации ограниченного распространения;

- при сообщениях антивирусных программ о выявленном вредоносном программном обеспечении немедленно сообщить ответственному за АРМ ДСП и системному администратору АРМ ДСП;

- использовать для работы на АРМ ДСП, только учтенные съемные машинные носители информации (компакт диски, флеш-накопители и т.д.), которые учитываются в Журнале учета машинных носителей информации, предназначенных для хранения и обработки служебной информации ограниченного распространения, ответственным за эксплуатацию АРМ ДСП;

- в случае необходимости использования съемных машинных носителей информации, провести проверку этих носителей на отсутствие вредоносного программного обеспечения;

- при наличии служебной необходимости копирования служебной информации ограниченного распространения на электронные носители информации выполнять копирование только на учтенные съемные машинные носители информации;

съемные машинные носители информации, содержащие служебную информацию ограниченного распространения, должны храниться в надежно запираемых хранилищах, обеспечивающих их физическую сохранность и недоступность для несанкционированного ознакомления;

при служебной необходимости создания на АРМ ДСП новых электронных документов, содержащих служебную информацию ограниченного распространения, пользователь создает и хранит такие документы в строго отведенном для этого каталоге, доступ к которому имеет только данный пользователь;

выполнять печать документов, содержащих служебную информацию ограниченного распространения, только на принтере, подключенном системным администратором АРМ ДСП;

в случае возникновения необходимости временно покинуть рабочее помещение во время работы на АРМ ДСП пользователь обязан выключить компьютер либо заблокировать его. При отсутствии в покидаемом помещении других служащих пользователь обязан закрыть дверь помещения на ключ или другой используемый ограничитель доступа;

при отсутствии необходимости работы на АРМ ДСП выключить его;

покидая рабочее помещение в конце рабочего дня, пользователь обязан выключить все средства вычислительной техники и закрыть дверь помещения на ключ;

немедленно выполнять предписания ответственного за эксплуатацию АРМ ДСП и системного администратора АРМ ДСП, предоставлять по их требованию АРМ ДСП для контроля и проверки.

2.4. При обработке служебной информации ограниченного распространения пользователю АРМ ДСП запрещается:

самостоятельно производить удаление, установку или настройку любого программного обеспечения;

оставлять АРМ ДСП без контроля;

допускать к включенному АРМ ДСП посторонних лиц;

запускать любые системные или прикладные программы, не входящие в состав программного обеспечения АРМ ДСП;

работать с неучтенными машинными носителями информации;

производить копирование защищаемой информации на неучтенные носители информации (в том числе и для временного хранения информации);

работать на АРМ ДСП с защищаемой информацией при обнаружении неисправностей;

несанкционированно выносить из помещений оборудование.

2.5. Пользователь АРМ ДСП несет персональную ответственность за соблюдение установленных требований во время работы на АРМ ДСП.

3. Требования к пользователю АРМ ДСП по сохранности пароля

3.1. Допуск пользователей к обработке служебной информации ограниченного распространения на АРМ ДСП осуществляется на основании идентификатора и личного пароля.

3.2. Первичные пароли доступа к АРМ ДСП устанавливаются системным администратором АРМ ДСП. Пользователь обязан сменить личный пароль, предоставленный системным администратором АРМ ДСП при первом входе в систему.

3.3. В случае смены личного пароля пользователь самостоятельно меняет его, руководствуясь правилами, указанными в п. 3.6.

3.4. Доведение до пользователей идентификаторов пользователей и личных паролей, осуществляет системный администратор АРМ ДСП.

3.5. Смена личного пароля должна производиться в обязательном порядке в следующих случаях:

- компрометации (подозрении на компрометацию) пароля;
- по инициативе системного администратора АРМ ДСП или ответственного за АРМ ДСП.

3.6. При формировании пароля необходимо руководствоваться следующими требованиями:

длина пароля должна быть не менее 8-и буквенно-цифровых символов;

пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации;

в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры;

запрещается использовать ранее использованные пароли.

3.7. При использовании пароля пользователю запрещается:

записывать свои пароли в очевидных местах (внутренности ящика стола, на мониторе ПЭВМ, на обратной стороне клавиатуры и т.д.);

хранить пароли в записанном виде на отдельных листах бумаги;

сообщать свои пароли посторонним лицам, а также сведения о применяемых средствах защиты от несанкционированного доступа на АРМ ДСП;

вводить личный пароль и другие учетные данные, если клавиатура находится в поле зрения других лиц.

Приложение 5

к Методическим рекомендациям по защите информации на автоматизированных рабочих местах, предназначенных для обработки служебной информации ограниченного распространения в органах исполнительной государственной власти области, государственных учреждениях области

ТИПОВАЯ ФОРМА

ТРЕБОВАНИЯ

к системе защиты информации автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения

В настоящем документе устанавливаются требования к системе защиты информационных ресурсов, содержащих служебную информацию ограниченного распространения, обрабатываемую на автоматизированных рабочих местах (далее – АРМ ДСП) в органах исполнительной государственной власти и государственных учреждениях Вологодской области для класса защищенности 1Г.

Настоящий документ разработан в соответствии с требованиями:

Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утвержден решением председателя Гостехкомиссии России от 30.03.1992 года.

Специальные требования и рекомендации по технической защите конфиденциальной информации (далее – СТР-К) Гостехкомиссии России 2001 год.

Требования к системе защиты АРМ ДСП определяются исходя из: характера обрабатываемой информации (перечня защищаемых информационных ресурсов и их уровня конфиденциальности);

условия ее эксплуатации (режима обработки данных в АРМ ДСП).

Автоматизированная обработка служебной информации ограниченного распространения допускается только на базе автономных АРМ ДСП или в локальных вычислительных сетях (далее – ЛВС), если ЛВС не имеет подключения к другим автоматизированным информационным системам.

Информационные ресурсы АРМ ДСП предназначены для обработки и (или) хранения служебной информации ограниченного распространения разных уровней конфиденциальности. АРМ ДСП относится к многопользовательской автоматизированной системе с разграничением прав доступа пользователей к обрабатываемой информации.

В соответствии с используемым в СТР-К порядком классификации

автоматизированных систем, в зависимости от вида обрабатываемых сведений конфиденциального характера наиболее близкой по типу к обрабатываемой на АРМ ДСП служебной информации ограниченного распространения является информация составляющую служебную тайну, и соответственно АРМ ДСП должны быть отнесены по уровню защищенности к классу не ниже 1Г.

Требования к классу защищенности 1Г:

Подсистемы и требования	Класс 1Г
1. Подсистема управления доступом	
1.1. Идентификация, проверка подлинности и контроль доступа субъектов:	
в систему	Да
к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ	Да
к программам	Да
к томам, каталогам, файлам, записям, полям записей	Да
2. Подсистема регистрации и учета	
2.1. Регистрация и учет:	
входа (выхода) субъектов доступа в (из) систему (узел сети)	Да
выдачи печатных (графических) выходных документов	Да
запуска (завершения) программ и процессов (заданий, задач)	Да
доступа программ субъектов доступа к защищаемым файлам, включая их создание и удаление, передачу по линиям и каналам связи	Да
доступа программ субъектов доступа к терминалам, ЭВМ, узлам сети ЭВМ, каналам связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям записей	Да
2.2. Учет носителей информации	Да
2.3. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей	Да
3. Криптографическая подсистема	Не требуется
4. Подсистема обеспечения целостности	
4.1. Обеспечение целостности программных средств и обрабатываемой информации	Да
4.2. Физическая охрана средств вычислительной техники и носителей информации	Да
4.3. Периодическое тестирование СЗИ НСД	+
4.4. Наличие средств восстановления СЗИ НСД	+
4.5. Использование сертифицированных средств защиты	Не требуется

1. Подсистема управления доступом:

– должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее восьми буквенно-цифровых символов;

– должна осуществляться идентификация терминалов, ЭВМ, узлов сети

ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;

- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

2. Подсистема регистрации и учета:

– должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

результат попытки входа: успешная или неуспешная - несанкционированная;

идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

код или пароль, предъявленный при неуспешной попытке;

– должна осуществляться регистрация выдачи печатных (графических) документов на "твердую" копию. В параметрах регистрации указываются:

дата и время выдачи (обращения к подсистеме вывода);

спецификация устройства выдачи [логическое имя (номер) внешнего устройства];

краткое содержание (наименование, вид, шифр, код) документа;

идентификатор субъекта доступа, запросившего документ;

– должна осуществляться регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:

дата и время запуска;

имя (идентификатор) программы (процесса, задания);

идентификатор субъекта доступа, запросившего программу (процесс, задание);

результат запуска (успешный, неуспешный - несанкционированный);

– должна осуществляться регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. 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;

– должна осуществляться регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам, ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, файлам, записям, полям

записей. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная - несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого объекта [логическое имя (номер)];
- должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку);
- учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема);
- должна осуществляться очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов).

3. Криптографическая подсистема:

не требуется.

4. Подсистема обеспечения целостности:

- должна быть обеспечена целостность программных средств СЗИ НСД, а также неизменность программной среды. При этом:
 - целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонент СЗИ;
 - целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;
- должна осуществляться физическая охрана СВТ (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;
- должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД;
- должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Приложение 6
к Методическим рекомендациям по
защите информации на
автоматизированных рабочих местах,
предназначенных для обработки
служебной информации ограниченного
распространения в органах
исполнительной государственной власти
области, государственных учреждениях
области

ТИПОВАЯ ФОРМА

Матрица доступа
к защищаемым информационным ресурсам автоматизированного рабочего
места, предназначенного для обработки служебной информации
ограниченного распространения

№	Субъект доступа	Права доступа к защищаемым информационным ресурсам
1	Системный администратор АРМ	Ч ¹ , Д ¹ , И ¹ , У ¹
2	Ответственный за эксплуатацию АРМ	Ч ¹ , Д ¹ , И ¹ , У ¹
3	Пользователь АРМ	Ч ¹ , Д ¹ , И ¹ , У ¹

Где:

Ч – чтение данных;

Д – добавление данных;

И – изменение данных;

У – удаление данных;

¹ – в пределах каталога, к которому имеет доступ конкретный пользователь.

Каждый пользователь имеет доступ к конкретному каталогу на жестком магнитном диске, определенному для него системным администратором АРМ ДСП.

Приложение 7
к Методическим рекомендациям по
защите информации на
автоматизированных рабочих местах,
предназначенных для обработки
служебной информации ограниченного
распространения в органах
исполнительной государственной власти
области, государственных учреждениях
области

ТИПОВАЯ ФОРМА

УТВЕРЖДАЮ

Руководитель органа исполнительной
государственной власти/государственного
учреждений области

____ И.О. Фамилия

« ____ » _____ 202__

АКТ

классификации автоматизированного рабочего места АРМ ДСП № __,
предназначенного для обработки служебной информации ограниченного
распространения

Комиссия в составе:

рассмотрев исходные данные на:

**автоматизированное рабочее место АРМ ДСП № __, предназначенное
для обработки служебной информации ограниченного
распространения**

условия его эксплуатации (режим работы – многопользовательский, с разными правами доступа пользователей к защищаемой информации), с учетом характера обрабатываемой информации (служебная тайна) и в соответствии с руководящими документами Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа информации. Классификация автоматизированных систем и требования по защите информации» и «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)»,

РЕШИЛА

Установить для:

автоматизированного рабочего места АРМ ДСП № __,

предназначенного для обработки служебной информации
ограниченного распространения,

Класс защищенности – 1Г.

Председатель комиссии:

И.О. Фамилия

Члены комиссии:

И.О. Фамилия

И.О. Фамилия

И.О. Фамилия

ЖУРНАЛ

учета машинных носителей информации, предназначенных для хранения и обработки служебной информации ограниченного распространения

[illegible]

Приложение 9
к Методическим рекомендациям по защите
информации на автоматизированных рабочих
местах, предназначенных для обработки
служебной информации ограниченного
распространения в органах исполнительной
государственной власти области, государственных
учреждениях области

ТИПОВАЯ ФОРМА

ЖУРНАЛ
регистрации работы на автоматизированном рабочем месте, предназначенном для обработки служебной
информации ограниченного распространения
АРМ ДСП № ____

Дата	Исполнитель	Время начала работы	Время окончания работы	Цель и описание проведенных работ	Подпись исполнителя	Подпись ответственного за эксплуатацию АРМ ДСП
1	2	3	4	5	6	7

Приложение 10
к Методическим рекомендациям по
защите информации на
автоматизированных рабочих местах,
предназначенных для обработки
служебной информации ограниченного
распространения в органах
исполнительной государственной власти
области, государственных учреждениях
области

ТИПОВАЯ ФОРМА

УТВЕРЖДАЮ

Руководитель органа исполнительной
государственной власти/государственного
учреждений области

_____ И.О. Фамилия

«__» _____ 202__

ПРОТОКОЛ

оценки эффективности реализованных мер по защите информации,
обрабатываемой на автоматизированном рабочем месте АРМ ДСП № __,
предназначенном для обработки служебной информации ограниченного
распространения

1. Общие положения

Настоящий документ разработан в соответствии с:

Руководящий документ. Автоматизированные системы. Защита от
несанкционированного доступа к информации. Классификация
автоматизированных систем и требования по защите информации. Утвержден
решением председателя Гостехкомиссии России от 30.03.1992 г.;

Требования к системе защиты информации автоматизированных рабочих
мест, предназначенных для обработки служебной информации ограниченного
распространения (далее – Требования к СЗИ АРМ ДСП). Утверждены приказом
_____ от «__» _____ 202__ года № _____.

В настоящем документе отражен перечень принятых мер, направленных на
защиту информации, обрабатываемой на автоматизированном рабочем месте
АРМ ДСП № __, предназначенном для обработки служебной информации
ограниченного распространения (далее – АРМ ДСП № __).

2. Объект оценки

Объект оценки: АРМ ДСП № __.

АРМ ДСП № ____ размещено в кабинете № ____ в здании, расположенном по адресу: г. Вологда, ул. _____, д. ____.

На момент проведения проверки АРМ ДСП № ____ находилось в работоспособном состоянии.

Перечень технических и программных средств АРМ ДСП № ____ представлен в Техническом паспорте АРМ ДСП № ____.

3. Оценка эффективности реализованных мер по защите информации, обрабатываемой на АРМ ДСП № ____

Оценка эффективности реализованных мер по обеспечению безопасности информации проводилась в соответствии с Актом классификации АРМ ДСП № ____ от « ____ » _____ 202 ____ г. (класс защищенности АРМ ДСП – 1Г) и Требованиями к СЗИ АРМ ДСП.

Требование к АРМ ДСП № ____	Реализация требования
1. ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ	
1.1. Идентификация и аутентификация (проверка подлинности) субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.	Механизмы идентификации и аутентификации: ОС _____
1.2. Идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам.	Механизмы идентификации и аутентификации: ОС _____
1.3. Идентификация программ, томов, каталогов, файлов, записей, полей записей по именам.	Механизмы идентификации и аутентификации: ОС _____
1.4. Контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.	Механизмы идентификации, аутентификации и защита данных: ОС _____; ПК _____
2. ПОДСИСТЕМА РЕГИСТРАЦИИ И УЧЕТА	
2.1. Регистрация входа/выхода субъектов доступа в систему/из системы, либо регистрация загрузки и инициализации операционной системы и ее программного останова. Регистрация выхода из системы или останова не проводится в моменты аппаратного отключения системы. В параметрах регистрации указываются: ○ время и дата входа/выхода субъекта доступа в систему/из системы или загрузки/останова системы; ○ результат попытки входа: успешная или неуспешная – несанкционированная; ○ идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа; ○ код или пароль, представленный при неуспешной попытке.	Механизмы аудита безопасности ОС _____
2.2. Регистрация выдачи печатных (графических) документов на «твердую» копию. Выдача должна сопровождаться автоматической маркировкой каждого листа (страницы) документа его последовательным номером, общим количеством листов (страниц) и	С помощью организационно-распорядительных мероприятий. Механизмы аудита безопасности ОС _____

учетными реквизитами АС. В параметрах регистрации указываются: - о время и дата выдачи (обращения к подсистеме вывода); - идентификатор устройства выдачи (логическое имя/номер); - краткое содержание (наименование, вид, шифр, код) и уровень конфиденциальности документа; - идентификатор субъекта доступа, запросившего документ.	
2.3. Регистрация запуска/завершения программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются: - дата и время запуска; - имя (идентификатор) программы (задания); - идентификатор субъекта доступа, запросившего программу (задания); - результат запуска (успешный, неуспешный – несанкционированный).	Механизмы аудита безопасности ОС
2.4. Регистрация попыток доступа программных средств (программ, заданий) к защищаемым файлам. 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.	Механизмы аудита безопасности ОС
2.5. Регистрация попыток доступа программных средств к следующим дополнительным защищаемым объектам доступа: терминалам ЭВМ, узлам сети ЭВМ, линиям (каналам) связи, внешним устройствам ЭВМ, программам, томам, каталогам, записям, полям записей. В параметрах регистрации указываются: - дата и время попытки доступа к защищаемому объекту с указанием ее результата: успешная, неуспешная – несанкционированная; - идентификатор субъекта доступа; - спецификация защищаемого объекта (логическое имя/номер).	Механизмы аудита безопасности ОС
2.6. Учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных в журнал (учетную карточку).	Реализуется с помощью организационно-распорядительных мероприятий. Ведется Журнал учета машинных носителей информации, предназначенных для хранения и обработки служебной информации ограниченного распространения, в котором регистрируются все машинные носители информации АС.
2.7. Учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).	Реализуется с помощью организационно-распорядительных мероприятий.
2.8. Очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ и внешних носителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных	Механизм безопасности защита данных пользователя ОС _____; Очистка внешних накопителей обеспечивается пользователями в соответствии с инструкциями и

(файлов).	должностными обязанностями.
3. ПОДСИСТЕМА ОБЕСПЕЧЕНИЯ ЦЕЛОСТНОСТИ	
3.1. Обеспечение целостности программных средств СЗИ НСД, а также неизменность программной среды, при этом: - целостность СЗИ НСД проверяется при загрузке системы по контрольным суммам компонентов СЗИ; - целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации.	Механизм безопасности защиты ФБО; Отсутствие на АРМ средств разработки исполняемых модулей программного обеспечения; Контроль целостности основных конфигурационных файлов ОС обеспечивается использованием программы контроля и настройки сертифицированных версий продуктов _____.
3.2. Физическая охрана средств вычислительной техники (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время.	Реализуется с помощью организационно-распорядительных мероприятий.
3.3. Периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест-программ, имитирующих попытки НСД	Механизмы тестирования ФБО; ОС _____; Антивирус _____; С помощью организационно-распорядительных мероприятий.
3.4. Наличие средств восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.	Средство резервного копирования и аварийного восстановления; С помощью организационно-распорядительных мероприятий.

Реализованные меры по обеспечению безопасности информации на АРМ ДСП № __ соответствуют требованиям, предъявляемым к автоматизированным системам класса защищенности 1Г.

ОЦЕНКУ ЭФФЕКТИВНОСТИ ПРОВЕЛИ:

_____ И.О. Фамилия

_____ И.О. Фамилия

_____ И.О. Фамилия

УТВЕРЖДЕНА

приказом Департамента цифрового
развития области

от «21» апреля 2023 г. № 38-О
(приложение 2)

ИНСТРУКЦИЯ

системного администратора автоматизированных рабочих мест,
предназначенных для обработки служебной информации ограниченного
распространения

1. Общие положения

1.1. Настоящая инструкция системного администратора автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения (далее – АРМ ДСП), определяет обязанности, полномочия и ответственность системного администратора АРМ ДСП по обеспечению бесперебойной работоспособности АРМ ДСП и технических средств защиты при обработке документов, содержащих служебную информацию ограниченного распространения.

1.2. Системными администраторами АРМ ДСП, ответственными за сопровождение, администрирование и техническую поддержку АРМ ДСП, являются работники бюджетного учреждения в сфере информационных технологий Вологодской области «Центр информационных технологий» (далее – БУ ВО «ЦИТ»).

1.3. Инструкция системного администратора АРМ ДСП (далее – Инструкция) устанавливает порядок сопровождения, администрирования и технической поддержки АРМ ДСП, в целях:

- обеспечения доступа пользователей, допущенных к автоматизированной обработке служебной информации ограниченного распространения в органе исполнительной государственной власти, государственном учреждении Вологодской области, к ресурсам АРМ ДСП в соответствии с их полномочиями;
- предотвращения несанкционированного доступа к служебной информации ограниченного распространения на АРМ ДСП;
- предотвращения несанкционированного уничтожения, искажения, копирования, блокирования служебной информации ограниченного распространения на АРМ ДСП.

1.4. В целях обеспечения сохранности и конфиденциальности служебной информации ограниченного распространения все действия по сопровождению, администрированию и технической поддержке АРМ ДСП, должны выполняться работниками БУ ВО «ЦИТ».

1.5. При первичном доступе к АРМ ДСП системные администраторы АРМ ДСП должны быть ознакомлены под подпись с данной Инструкцией и иными организационно-распорядительными документами, регламентирующими

обработку служебной информации ограниченного распространения на АРМ ДСП.

2. Права и обязанности системного администратора АРМ ДСП

2.1. Системный администратор АРМ ДСП обязан знать и выполнять требования действующих нормативных и руководящих документов, а также внутренних инструкций и распоряжений, регламентирующих порядок действий по защите информации ограниченного распространения.

2.2. Все действия системного администратора АРМ ДСП в отношении АРМ ДСП подлежат фиксации в Журнале регистрации работы на АРМ ДСП.

2.3. Обеспечивать установку, настройку и своевременное обновление: средств вычислительной техники, входящих в состав АРМ ДСП; программного обеспечения АРМ ДСП;

аппаратных и программных технических средств защиты.

2.4. Не допускать физическое воздействие на технические средства АРМ ДСП, в результате которого может быть нарушено их функционирование.

2.5. Обеспечивать работоспособность средств вычислительной техники, входящих в состав АРМ ДСП.

2.6. Обеспечивать функционирование и поддерживать работоспособность средств защиты информации.

2.7. В случае отказа работоспособности технических средств и программного обеспечения АРМ ДСП, в том числе средств защиты информации, принимать меры по их своевременному восстановлению и выявлению причин, приведших к отказу работоспособности.

2.8. Не реже одного раза в месяц обновлять базы антивирусного программного обеспечения.

2.9. По заявке пользователя осуществлять на АРМ ДСП регистрацию новых пользователей, генерацию идентификаторов пользователей и личных паролей, создавать для них каталоги, доступ, к которому имеет только данные пользователи. Не передавать никому кроме пользователя АРМ ДСП сгенерированные учетные данные пользователей и их пароли.

2.10. Обеспечивать строгое выполнение требований по обеспечению безопасности информации при организации обслуживания технических и программных средств АРМ ДСП.

2.11. Принимать меры по реагированию в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий.

2.12. Системному администратору АРМ ДСП запрещается:

Допускать к включенному АРМ ДСП посторонних лиц.

Подключать к АРМ ДСП сторонние устройства, отсутствующие в Журнале учета машинных носителей информации, предназначенных для хранения и обработки служебной информации ограниченного распространения.

Несанкционированно выносить из помещений оборудование.

2.13. Системный администратор АРМ ДСП имеет право:

Требовать прекращения обработки конфиденциальной информации, как в

целом, так и для отдельных пользователей, в случае выявления нарушений установленного порядка работ или нарушения функционирования АРМ ДСП или технических средств защиты.

Присутствовать при выполнении технического обслуживания элементов АРМ ДСП сторонними физическими лицами и организациями.

Требовать от пользователей АРМ ДСП исполнения своих обязанностей в соответствии с инструкцией пользователя автоматизированного рабочего места, предназначенного для обработки служебной информации ограниченного распространения.

В случае подозрения на неисправность технических средств и/или программного обеспечения АРМ ДСП, а также в случае заражения АРМ ДСП вредоносным программным обеспечением требовать от пользователей АРМ ДСП немедленно прекратить работу и предоставить АРМ ДСП для проверки.

3. Требования к паролям

3.1. При формировании пароля необходимо руководствоваться следующими требованиями:

3.2. Длина пароля должна быть не менее 8-и буквенно-цифровых символов.

3.3. Пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, дни рождения и другие памятные даты, номера телефонов, автомобилей, адреса места жительства, наименования АРМ, общепринятые сокращения) и другие данные, которые могут быть подобраны злоумышленником путем анализа информации.

3.4. В числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, а также цифры.

3.5. Запрещается повторно использовать ранее сгенерированные пароли.

4. Ответственность

4.1. За разглашение служебной информации ограниченного распространения, ее распространение без санкции должностного лица, имеющего данные полномочия, нарушение порядка обращения с документами или материальными носителями, содержащими такую информацию, системный администратор АРМ ДСП может быть привлечен к дисциплинарной или иной предусмотренной законодательством ответственности.

УТВЕРЖДЕНО

приказом Департамента цифрового
развития области

от «21» апреля 2023 г. № ЗР-0
(приложение 3)

ПОЛОЖЕНИЕ

**о Реестре автоматизированных рабочих мест, предназначенных для
обработки служебной информации ограниченного распространения в
органах исполнительной государственной власти области, государственных
учреждениях области**

Настоящее Положение устанавливает порядок формирования и ведения реестра автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения в органах исполнительной государственной власти области, государственных учреждениях области (далее - Реестр), состав включаемых в него сведений и порядок предоставления таких сведений.

Ведение Реестра осуществляет бюджетное учреждение в сфере информационных технологий Вологодской области «Центр информационных технологий» в электронном виде. БУ ВО «ЦИТ» определяет должностных лиц, ответственных за включение сведений в реестр и исключение сведений из него.

В реестр включается следующая информация:

- наименование объекта учета;
- инвентарный номер;
- наименование организации;
- фамилия, имя, отчество, должность лица, ответственного за эксплуатацию автоматизированного рабочего места, предназначенного для обработки служебной информации ограниченного распространения;
- место установки автоматизированного рабочего места;
- операционная система, установленная на АРМ;
- Ф.И.О. системного администратора;
- средство антивирусной защиты (АВЗ), установленное на АРМ.

Формирование реестра осуществляется путем включения в него сведений об объектах по форме согласно приложению.

В случае изменения данных автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения, орган исполнительной государственной власти области, государственное учреждение должно внести изменения в пакет документов и согласовать их с БУ ВО «ЦИТ», после чего отдел защиты информации БУ ВО «ЦИТ» в течение 5 рабочих дней вносит в реестр актуальные сведения.

В случае принятия решения о прекращении (приостановке) обработки на автоматизированном рабочем месте служебной информации ограниченного распространения орган исполнительной государственной власти области, государственное учреждение обязано уведомить об этом БУ ВО «ЦИТ», после

чего отдел защиты информации БУ ВО «ЦИТ» в течение 5 рабочих дней исключает сведения об объекте из реестра.

Сведения об объектах, включенные в реестр, предоставляются органам исполнительной государственной власти области, государственным учреждениям области по запросу. Сведения предоставляются органам исполнительной государственной власти области, государственным учреждениям области в виде выписки только в отношении эксплуатируемых ими автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения.

PEECTP

автоматизированных рабочих мест, предназначенных для обработки служебной информации ограниченного распространения в органах исполнительной государственной власти области, государственных учреждениях области

[illegible]