ПРАВИТЕЛЬСТВО АРХАНГЕЛЬСКОЙ ОБЛАСТИ

**МИНИСТЕРСТВО СВЯЗИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ АРХАНГЕЛЬСКОЙ ОБЛАСТИ**

# РАСПОРЯЖЕНИЕ

от 04 июля 2016 года № 21-р

г. Архангельск

**Об утверждении регламента предоставления услуг по аудиту информационных систем пользователей в системе исполнительных органов государственной власти Архангельской области**

В соответствии со статьей 18.1 Федерального закона от 27 июля 2006 года № 152-ФЗ «О персональных данных», Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», постановлением Правительства Российской Федерации от 01 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

1. Утвердить прилагаемый регламент предоставления услуг по аудиту информационных систем пользователей в системе исполнительных органов государственной власти Архангельской области (далее – регламент).

2. Руководителю государственного автономного учреждения Архангельской области «Управление информационно-коммуникационных технологий Архангельской области» обеспечить размещение утвержденного регламента на сайте государственного автономного учреждения Архангельской области «Управление информационно-коммуникационных технологий Архангельской области» в информационно-телекоммуникационной сети «Интернет» (http://www.ict29.ru) в течение 15 дней с момента подписания настоящего распоряжения.

**Министр** **Н.П. Родичев**

УТВЕРЖДЕН
распоряжением министерства связи
и информационных технологий
Архангельской области
от 04 июля 2016 года № 21-р

# РЕГЛАМЕНТ
# предоставления услуг по аудиту информационных систем пользователей

## I. Предмет регулирования регламента

1. Настоящий регламент устанавливает порядок предоставления услуг по аудиту информационных систем пользователей (далее – услуги) и стандарт предоставления услуг, включая сроки и последовательность процедур и действий при осуществлении полномочий по предоставлению услуг.

2. Целью услуг является проверка достаточности и полноты принятых технических и организационных мер по защите информации в организации, за исключением мер по защите сведений, составляющих государственную тайну.

3. Объектами услуг являются:

средства вычислительной техники, на которых обрабатывается информация ограниченного доступа, кроме сведений, составляющих государственную тайну;

соблюдение требований законодательства Российской Федерации в области защиты информации ограниченного доступа, кроме сведений, составляющих государственную тайну.

4. Предоставление услуг включает в себя административные процедуры:

формирование и утверждение ежегодного плана предоставления услуг;

направление информационных писем и программ проверяемым организациям;

предоставление услуг и подготовка отчета по результатам их выполнения;

методическая и консультационная помощь при выполнении рекомендаций, содержащихся в отчете по результатам предоставления услуг.

5. Блок-схема предоставления услуг приведена в приложении № 1 к настоящему регламенту.

## II. Описание исполнителей и заявителей при предоставлении услуг

6. Предоставление услуг осуществляется государственным автономным учреждением Архангельской области «Управление

информационно-коммуникационных технологий Архангельской области» (далее – проверяющая организация). Проверяющая организация должна иметь следующие лицензии:

лицензию Федеральной службы по техническому и экспортному контролю Российской Федерации (далее – ФСТЭК России) на деятельность по технической защите конфиденциальной информации, в перечне работ и услуг которой значится пункт – контроль защищенности конфиденциальной информации от несанкционированного доступа и ее модификации в средствах и системах информатизации.

лицензию Федеральной службы безопасности Российской Федерации (далее – ФСБ России) на осуществление деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя).

## III. Стандарт предоставления услуг

7. Услуги предоставляются рабочей группой проверяющей организации (далее – рабочая группа), назначаемой приказом руководителя проверяющей организации. В рабочую группу по согласованию сторон, участвующих в предоставлении услуг, могут быть включены сторонние специалисты.

8. Предоставление услуг осуществляется в соответствии со следующими основными нормативно-правовыми актами:

8.1. Конституция Российской Федерации;

8.2. Федеральный закон от 30 декабря 2001 года № 197-ФЗ «Трудовой кодекс Российской Федерации»;

8.3. Федеральный закон от 27 июля 2004 года № 79-ФЗ «О государственной гражданской службе Российской Федерации»;

8.4. Федеральный закон от 30 декабря 2001 года № 195-ФЗ «Кодекс российской федерации об административных правонарушениях»;

8.5. Федеральный закон от 04 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности»;

8.6. Федеральный закон от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

8.7. Федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

8.8. Федеральный закон от 27 июля 2010 года № 210-ФЗ «Об организации предоставления государственных и муниципальных услуг»;

8.9. Федеральный закон Российской Федерации от 18 декабря 2006 года № 230-ФЗ «Гражданский кодекс Российской Федерации». Часть 4;

8.10. Федеральный закон от 06 апреля 2011 года № 63-ФЗ «Об электронной подписи»;

8.11. Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

8.12. Постановление Правительства РФ от 15 сентября 2008 года № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»;

8.13. Постановление Правительства РФ от 21 марта 2012 года № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

8.14. Приказ ФСТЭК России от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

8.15. Приказ ФСТЭК России от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

8.16. Приказ ФСБ России от 10 июля 2014 года № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

8.17. Специальные требования и рекомендации по технической защите конфиденциальной информации, утверждены приказом Гостехкомиссии России от 30 августа 2002 года № 282.

## IV. Условия, необходимые для оказания услуг

9. Для оказания услуг проверяемая организация предоставляет проверяющей организации доступ в здания и помещения, доступ к информационно-коммуникационной инфраструктуре, организационно-распорядительную, эксплуатационную и техническую документацию согласно Перечню документов, приведенному в приложении № 2 к настоящему регламенту.

## V. Сроки оказания услуг

10. Сроки выполнения отдельных процедур и действий:

10.1. Формирование и утверждение ежегодного плана предоставления услуг – не позднее 31 декабря года, предшествующего году, в котором будут предоставляться услуги;

10.2. Направление информационных писем проверяемым организациям – не позднее, чем за 7 календарных дней до даты начала предоставления услуг;

10.3. Предоставление услуг и подготовка отчета – в течение не более чем 60 календарных дней со дня выполнения условий, необходимых для предоставления услуг;

10.4. Консультационная помощь при выполнении рекомендаций, содержащихся в отчете по результатам предоставления услуг – в течение 14 календарных дней со дня поступления запроса от проверяемой организации.

## VI. Основания для приостановления или отказа в предоставлении услуг

11. Основанием для приостановления предоставления услуг является несоблюдение проверяемой организацией пункта 10 настоящего регламента. В этом случае проверяющая организация в письменном виде уведомляет проверяемую организацию о невозможности предоставления услуг с указанием причин.

## VII. Результаты предоставления услуг

12. Результатом предоставления услуг является отчет о проведении аудита информационных систем в проверяемой организации. Примерная структура и содержание отчета приведены в приложении № 3 к настоящему регламенту. Структура и содержание отчета могут изменяться

по усмотрению проверяющей организации для наилучшего достижения целей проведения услуг.

13. Отчет оформляется на бумажном носителе с пометкой «Для служебного пользования» в двух экземплярах. Первый экземпляр отчета направляется в адрес проверяемой организации, второй, по согласованию, в администрацию Губернатора Архангельской области и Правительства Архангельской области.

## VIII. Предоставление услуг и подготовка отчета

14. В ходе проведения услуг рабочая группа выполняет следующие мероприятия:

14.1. Направление информационного письма с уведомлением о начале и сроках проведения услуг.

В письме, направляемом на имя руководителя проверяемой организации, указываются сроки начала предоставления услуг в соответствии с утвержденным планом, ссылка на настоящий регламент, размещенный в сети «Интернет», сроки проведения услуг, копия приказа проверяющей организации о создании рабочей группы для предоставления услуг, просьба о назначении ответственного за взаимодействие с рабочей группой и контактные данные для обратной связи. Ответ на письмо проверяемой организацией предоставляется в бумажном виде или через систему электронного документооборота «Дело». Копия ответа направляется в электронном виде по адресу электронной почты, указанной в исходном письме. Сроки проведения услуг могут быть перенесены по взаимному согласию сторон. Перенос сроков фиксируется письмами за подписями руководителей проверяющей и проверяемой организации.

14.2. Проведение организационного совещания назначается по взаимному согласованию проверяющей и проверяемой организациями. В рамках совещания до руководства и сотрудников проверяемой организации доводятся цели и сроки проведения услуг, перечень документов, предоставляемых в соответствии с приложением № 2, обсуждаются иные организационные вопросы.

14.3. Анализ учредительных документов и проектно-технической, эксплуатационной и правоустанавливающей документации на здания (помещения), где размещаются элементы информационных систем, а также проектно-техническая и эксплуатационная документация на инженерно-технические коммуникации.

В ходе проведения анализа определяется географическое местоположение проверяемой организации и ее филиалов, основные виды деятельности, общее описание зданий, помещений, в которых располагается проверяемая организация, рассматриваются контролируемые зоны, в пределах которых обрабатывается информация ограниченного доступа. Результаты включаются в 4 и 5 разделы отчета (приложение № 3).

14.4. Анализ организационно-распорядительной документации проверяемой организации.

В ходе проведения анализа рабочей группой производится экспертная оценка применяемых организационных мер на соответствие требованиям нормативно-правовых актов по защите информации ограниченного доступа, указанных в пункте 7 настоящего регламента. Результаты анализа оформляется в виде таблицы соответствия или несоответствия анализируемого документа тому или иному пункту нормативно-правового акта и включаются в 7 раздел отчета (приложение № 3).

14.5. Анализ технических средств и программного обеспечения, применяемых в составе информационных систем проверяемой организации.

Анализ проводится с целью определения применяемых в процессе обработки информации основных технических средств, программного обеспечения и его версий, а также для сбора статистической информации о сроках эксплуатации применяемого оборудования, определение его морального износа, выявления случаев использования нелицензионного программного обеспечения. Анализ осуществляется сертифицированным программным обеспечением «Агент Инвентаризации» при взаимодействии с администраторами локальной вычислительной сети (далее – ЛВС) проверяемой организации. Сбор информации осуществляется в автоматизированном режиме, например с помощью групповых политик домена проверяемой организации, либо в ручном режиме запуском программного обеспечения на каждом рабочем месте и сервере. Результаты оформляются в виде списка оборудования и программного обеспечения с привязкой их к рабочей станции, мобильному рабочему месту или серверу и включаются в 6 раздел отчета (приложение № 3).

14.6. Анализ организации сетевого взаимодействия и выявление уязвимостей в информационных системах проверяемой организации.

Анализ проводится с целью определения порядка взаимодействия внутри информационных систем проверяемой организации, взаимодействия с другими информационными системами, в том числе внешними информационными системами, а также выявление уязвимостей программного обеспечения информационных систем, таких как:

ошибки проектирования сетевой инфраструктуры, которые позволяют проводить следующие атаки вида ARP Spoofing, DNS Spoofing, перехват, перенаправления сетевого трафика, реализация атаки MITM (человек-в-середине);

ошибки настройки коммутационного оборудования и системных сервисов (пароли по-умолчанию, небезопасные конфигурации);

использование устаревших или небезопасных сетевых протоколов, в том числе протоколов управления сетевым оборудованием;

недостатки разделения прав доступа на критичных с точки зрения безопасности узлах сети, возможность прослушивания трафика в ключевых точках сети с пользовательских узлов;

несанкционированные или неконтролируемые каналы выхода во внешние сети, несанкционированные каналы между сегментами сети;

недостатки управления обновлениями операционных систем на узлах и коммутационном оборудовании.

В процессе выявления уязвимостей применяется аппаратное и программное обеспечение, которое, по мнению рабочей группы, наиболее полно позволит реализовать цели анализа. Результаты включаются в 8 раздел отчета (приложение № 3).

14.7. Заключение по результатам проведения аудита.

В заключении описываются выявленные нарушения применяемых организационных и технических мер по защите информации действующему законодательству в области информационной безопасности, выявленные уязвимости, рекомендации и способы по их устранению. При выявлении нарушения законодательства должны указываться номер, дата, наименование и пункт нарушаемого нормативно-правового акта, а также ответственность, предусмотренная законодательством Российской Федерации. Заключение включается в 9 раздел отчета (приложение № 3).

## IX. Показатели доступности и качества услуг

15. Показателем доступности услуг является возможность проверяемой организации, в соответствие с п.20 настоящего Регламента, заявиться на предоставление услуги.

16.Показателями качества услуг являются:

отсутствие случаев нарушения сроков при предоставлении услуг;

отсутствие случаев удовлетворения в судебном порядке заявлений проверяемых организаций, оспаривающих действия (бездействие) проверяющей организации.

## X. Порядок разрешения разногласий

17. Все споры и разногласия, возникающие между проверяющей и проверяемой организациями при предоставлении услуг, разрешаются путем переговоров.

18. В случае невозможности разрешения споров и разногласий путем переговоров они передаются на рассмотрение в Арбитражный суд Архангельской области.

## XI. Формирование и утверждение ежегодного плана предоставления услуг

19. Включение организаций в ежегодный план предоставления услуг осуществляется проверяющей организацией по согласованию

с министерством связи и информационных технологий Архангельской области.

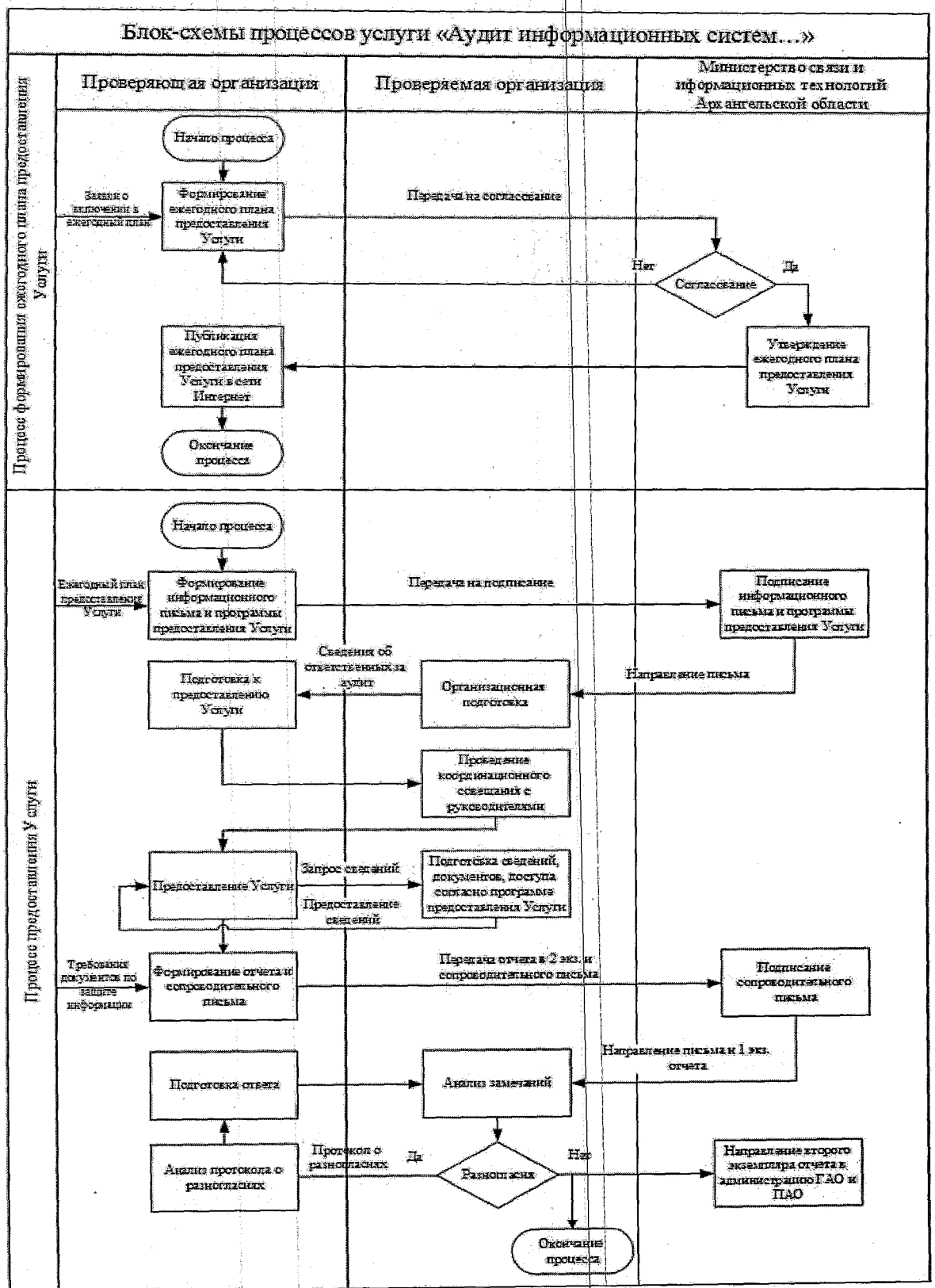
20. Проверяемые организации могут быть включены в план по собственной инициативе при условии направления официального письма в адрес проверяющей организации не позднее 31 октября года, предшествующего году, в котором будет предоставляться услуг.

21. План содержит, в том числе сведения о предполагаемой дате начала предоставления Услуги.

22. Ежегодный план предоставления услуг утверждается министерством связи и информационных технологий Архангельской области.

ПРИЛОЖЕНИЕ № 1

**Блок-схема предоставления услуг по аудиту информационных систем пользователей**



ПРИЛОЖЕНИЕ № 2

**Перечень документов, предоставляемых проверяемой организацией**

1. Учредительные документы.
2. Проектно-техническая, эксплуатационная и правоустанавливающая документация на здания (помещения), где размещаются элементы информационных систем, а также проектно-техническая и эксплуатационная документация на инженерно-технические коммуникации.
3. Документы, связанные с организационной структурой организации, положения об отделах.
4. Организационно-распорядительная документация по защите информации ограниченного доступа, за исключением сведений, составляющих государственную тайну.
5. Техническая документация на информационные системы.
6. Структурная схема информационных систем с указанием размещения их элементов.
7. Эксплуатационная и правоустанавливающая документация на средства вычислительной техники, эксплуатируемые в составе информационных систем.
8. Эксплуатационная и правоустанавливающая документация на системное и прикладное программное обеспечение, включая средства защиты информации, установленные в информационных системах.
9. Перечень сотрудников, участвующих в обработке информации ограниченного доступа, их роли и возможности, должностные (функциональные обязанности), фамилия и инициалы.

ПРИЛОЖЕНИЕ № 3

**Основные пункты отчета по результатам проведения аудита**

1. Основные понятия и определения.
2. Обозначения и сокращения.
3. Общие сведения о проверяемой организации.
4. Описание физического доступа, определение контролируемых зон.
5. Объекты информатизации.
6. Структура локальной вычислительной сети.
7. Организация защиты информации.
8. Сетевое взаимодействие и выявление уязвимостей.
9. Заключение по результатам проведения аудита.
10. Список законов и нормативных документов.