МИНИСТЕРСТВО АГРОПРОМЫШЛЕННОГО КОМПЛЕКСА
И РАЗВИТИЯ СЕЛЬСКИХ ТЕРРИТОРИЙ УЛЬЯНОВСКОЙ ОБЛАСТИ

РАСПОРЯЖЕНИЕ

29.05.2020 № 377

Экз.№ _____

г.Ульяновск

Об организации работы по защите информации, не содержащей сведений, составляющих государственную тайну, в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

В целях организации работы по защите информации, не содержащей сведений, составляющих государственную тайну, в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации, в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и во исполнение приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» утвердить:

1. Положение об использовании локальной вычислительной сети в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 1).

2. Порядок эксплуатации средств криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 2).

3. Порядок доступа в помещения, где размещены используемые Министерством агропромышленного комплекса и развития сельских территорий Ульяновской области и его подведомственной организацией средства криптографической защиты информации (приложение № 3).

4. Порядок доступа в помещения Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации, в которых ведётся обработка персональных данных (приложение № 4).

5. Порядок технического обслуживания, ремонта, модернизации технических и программных средств, входящих в состав информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (приложение № 5).

6. Порядок выявления инцидентов информационной безопасности в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 6).

7. Инструкцию по восстановлению связи в случае компрометации действующих ключей к средствам криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 7).

8. Инструкцию пользователя информационных систем Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (приложение № 8).

9. Инструкцию администратора информационной безопасности информационных систем Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (приложение № 9).

10. Инструкцию по организации парольной защиты при работе с информационными системами и устройствами в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 10).

11. Инструкцию по антивирусной защите информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (приложение № 11).

12. Инструкцию по резервному копированию данных информационных систем в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 12).

13. Инструкцию по защите информации от утечки по техническим каналам в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 13).

14. Список помещений, выделенных для установки сертифицированных средств криптографической защиты информации и хранения ключевых документов к ним, съёмных носителей электронной подписи, а также обработки персональных данных в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 14).

15. Форму журнала учёта опечатывания помещений, где размещены средства криптографической защиты информации, используемые Министерством агропромышленного комплекса и развития сельских

территорий Ульяновской области и подведомственной ему организации (приложение № 15).

16. Форму журнала технический (аппаратный) Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 16).

17. Форму журнала учёта носителей персональных данных, обрабатываемых в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 17).

18. Форму журнала учёта работ в серверном помещении Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (приложение № 18).

19. Форму журнала учёта проверок в области информационных технологий и защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (приложение № 19).

20. Форму журнала учёта журналов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации в рамках организации защиты информации (Приложение № 20).

Заместитель Председателя Правительства
Ульяновской области - Министр
агропромышленного комплекса и развития
сельских территорий Ульяновской области М.И.Семёнкин

Лист согласования
проекта распоряжения Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области
«Об организации работы по защите информации, не содержащей сведений, составляющих государственную тайну, в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации»

Проект внесён «___»_____ 2020 г.

Дата и время		Наименование должности	Подпись	Расшифровка подписи
Поступления	согласования			
		Заместитель Министра агропромышленного комплекса и развития сельских территорий Ульяновской области		М.С.Еварестова
		Заместитель Министра агропромышленного комплекса и развития сельских территорий Ульяновской области		И.В.Снежинская
		Директор департамента финансов – главный бухгалтер Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области		Т.А.Черкасова
		Директор департамента лицензирования, пищевой и перерабатывающей промышленности Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области		Д.А.Москвина
		Директор департамента проектного управления и цифровой экономики Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области		О.В. Игнатьева
		Начальник отдела правовой и организационной работы Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области		И.Н.Тимохин
		Референт департамента растениеводства, механизации и химизации Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области		С.А.Антонова
		Референт департамента животноводства, племенного дела и аквакультуры Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области		А.Н.Шаронин

		Директор ОГБУ «Агентство по развитию сельских территорий Ульяновской области»		Р.Р.Покров

Исполнитель: начальник отдела информационных технологий и защиты информации ОГБУ «Агентство по развитию сельских территорий Ульяновской области» О.В. Маркелов, 73-56-79

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к проекту распоряжения Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области «Об организации работы по защите информации, не содержащей сведений, составляющих государственную тайну, в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации»

Проект распоряжения Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области «Об организации работы по защите информации, не содержащей сведений, составляющих государственную тайну, в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации» (далее – проект распоряжения) разработан в целях организации работы по защите информации, не содержащей сведений, составляющих государственную тайну, в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и подведомственной ему организации, в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и во исполнение приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

Проектом распоряжения утверждаются организационно-распорядительные документы в рамках организации работы по защите информации, не содержащей сведений, составляющих государственную тайну, в Министерстве и подведомственной ему организации.

Начальник отдела информационных технологий
и защиты информации
ОГБУ «Агентство по развитию сельских
территорий Ульяновской области» О.В. Маркелов

ЛИСТ РАССЫЛКИ

проекта распоряжения Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области «Об организации работы по защите информации, не содержащей сведений, составляющих государственную тайну, в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации»

Адресат (Ф.И.О., должность)	Кол-во экз.	№ экз.	Почтовый адрес
Еварестова М.С., заместитель Министра агропромышленного комплекса и развития сельских территорий Ульяновской области	1	1	432011, г. Ульяновск, ул. Радищева, 5
Снежинская Н.В., заместитель Министра агропромышленного комплекса и развития сельских территорий Ульяновской области	1	2	432011, г. Ульяновск, ул. Радищева, 5
Черкасова Т.А., директор департамента финансов — главный бухгалтер Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области	1	3	432011, г. Ульяновск, ул. Радищева, 5
Москвина Д.А., директор департамента лицензирования, пищевой и перерабатывающей промышленности Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области	1	4	432011, г. Ульяновск, ул. Радищева, 5
Игнатьева О.В., директор департамента проектного управления и цифровой экономики Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области	1	5	432011, г. Ульяновск, ул. Радищева, 5
Тимохин И.Н., начальник отдела правовой и организационной работы Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области	1	6	432011, г. Ульяновск, ул. Радищева, 5
Антонова С.А., референт департамента растениеводства, механизации и химизации Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области	1	7	432011, г. Ульяновск, ул. Радищева, 5
Шаронин А.Н., референт департамента животноводства, племенного дела и аквакультуры Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области	1	8	432011, г. Ульяновск, ул. Радищева, 5
Покров Р.Р., директор ОГБУ «Агентство по развитию сельских территории Ульяновской области»	1	9	432011, г. Ульяновск, ул. Радищева, 5

Всего подлежит рассылке 9 экз.

Реестр составил: Маркелов О.В., телефон 73-56-79

Передано в рассылку _____

ПРИЛОЖЕНИЕ № 1

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29. 05. 2020 № 371

ПОЛОЖЕНИЕ
об использовании локальной вычислительной сети в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

1. Общие положения

1.1. Положение об использовании локальной вычислительной сети в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (далее - Положение) определяет структуру и состав локальной вычислительной сети (далее – ЛВС), условия и порядок подключения к ЛВС и ее использования в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и подведомственной ему организации (далее – подведомственная организация).

1.2. Настоящее Положение разработано в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Федеральным законом от 09.02.2009 № 8-ФЗ «Об обеспечении доступа к информации о деятельности государственных органов и органов местного самоуправления» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения в области использования ЛВС.

1.3. Для целей настоящего Положения используется следующие понятия:

ЛВС - распределенная система взаимосвязанных персональных компьютеров (рабочих станций сети), серверов, коммутационного оборудования, структурированной кабельной сети и других средств вычислительной техники.

Защищённая ЛВС (далее – ЗЛВС) – защищенный сегмент ЛВС, предназначенный для обработки информации ограниченного доступа.

Оператор ЛВС – областное государственное бюджетное учреждение «Агентство по развитию сельских территорий Ульяновской области» (далее - Агентство).

Администратор ЛВС – структурное подразделение Агентства, использующее ЛВС, ответственное за функционирование ЛВС,

администрирование ЛВС к информационно-телекоммуникационной сети «Интернет», распределение прав доступа в ЛВС.

Локальный администратор – сотрудник Агентства, использующий ЛВС, ответственный за функционирование рабочих станций в установленном штатном режиме работы.

Пользователь - сотрудник Министерства или подведомственной организации, а также лицо, имеющее доступ к информационным, программным и аппаратным ресурсам ЛВС.

Аппаратный ресурс - внутреннее или внешнее устройство хранения, обработки или передачи информации.

Информационный ресурс - сведения (сообщения, данные), входящие в состав отдельных документов, массивов документов, баз данных, представленные в электронно-цифровой форме.

Программный ресурс - системное или прикладное программное обеспечение.

Несанкционированный доступ к информации - доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

1.4. ЛВС предназначена для обеспечения доступа Пользователей к индивидуальным, общим или групповым информационным и техническим ресурсам сети, обеспечения коммуникаций пользователей друг с другом, обработки и хранения открытой информации и (или) информации ограниченного доступа при наличии ЗЛВС. ЛВС может включать в себя ресурсы и предоставлять их другим лицам на основе договоров об информационном взаимодействии в соответствии с действующими нормативными правовыми актами Российской Федерации.

2. Структура и состав ЛВС

2.1. Физической средой передачи информации в ЛВС служит структурированная кабельная система здания или отдельно проложенные кабели. Технология передачи данных - Ethernet (Fast Ethernet). Унифицированная аппаратная база позволяет обеспечивать одновременное функционирование на общем сетевом оборудовании и кабельной сети нескольких виртуальных логических сетей. Активное коммутационное оборудование ЛВС, серверы и рабочие станции питаются от отдельной сети гарантированного электроснабжения.

2.2. ЛВС образуют следующие базовые компоненты оборудования и программного обеспечения (программно-аппаратные ресурсы):

2.2.1. Серверы: файловые, баз данных, приложений, электронной почты, архивные, удаленного доступа, антивирусной защиты;

2.2.2. Телекоммуникационная инфраструктура: кабели, соединительные устройства, устройства расширения (и ограничения) доступа;

2.2.3. Рабочие станции (персональные компьютеры) Пользователей;

2.2.4. Системы бесперебойного питания серверов и рабочих станций;

2.2.5. Системы резервного копирования и хранения информации;

2.2.6. Информационная инфраструктура: сетевые операционные системы, средства защиты от несанкционированного доступа к информации, прикладное программное обеспечение коллективного доступа (правовые базы, геоинформационные системы, информационные и информационно-справочные системы, базы и хранилища данных, средства аналитической обработки данных и т.д.), программное обеспечение рабочих станций;

2.2.7. Периферийные устройства (принтеры, сканеры, многофункциональные устройства и др.).

3. Обязанности Оператора и Пользователей ЛВС

3.1. Оператор ЛВС обеспечивает:

3.1.1. Предоставление Пользователям ЛВС доступа к информационным ресурсам ЛВС в рамках единого информационно-коммуникационного пространства (электронная почта, справочные базы данных, справочно-правовые системы, регламентированный доступ к сетям общего пользования и другим ресурсам).

3.1.2. Принятие мер по защите информации, в том числе от несанкционированного доступа.

Защита информации обеспечивается:

предотвращением несанкционированного доступа к информации и (или) передачи её лицам, не имеющим права на доступ к информации;

своевременным обнаружением фактов несанкционированного доступа к информации;

предупреждением возможности неблагоприятных последствий нарушения порядка доступа к информации;

недопущением воздействия на технические средства обработки информации, в результате которого нарушается их функционирование;

возможностью незамедлительного восстановления работоспособности информационной системы;

постоянным контролем за обеспечением уровня защищённости информации.

3.1.3. Выдачу учётных данных (паролей, идентификаторов и т.п.) и уровня доступа к ресурсам ЛВС.

3.2. Пользователь обязан:

3.2.1. Предпринять все необходимые меры для недопущения утраты (разглашения) учётных данных (паролей, идентификаторов и т.п.). Передача Пользователем учётных данных иным Пользователям, а также посторонним лицам запрещена. В случае утраты своих учётных данных Пользователь обязан незамедлительно после обнаружения утраты уведомить об этом Оператора ЛВС.

3.2.2. При работе на рабочей станции выполнять только служебные задания.

3.2.3. При сообщениях тестовых программ о появлении вредоносного программного обеспечения незамедлительно сообщать об этом Администратору ЛВС.

3.2.4. При применении внешних носителей информации перед началом работы провести их проверку на предмет отсутствия вредоносного программного обеспечения.

3.2.5. При работе с информацией использовать только учтённые носители информации.

3.2.6. Выполнять требования Администратора ЛВС, связанные с соблюдением настоящего раздела.

3.2.7. Сохранять пароли в тайне, не сообщать их другим лицам.

3.2.8. Вводить личные пароли и другие учётные данные, убедившись, что клавиатура находится вне поля зрения других лиц.

3.2.9. Не реже 1 раза в месяц проводить смену пароля учётной записи пользователя в домене, в случае применения доменной структуры.

3.2.10. В случае обнаружения сбоя в работе рабочей станции, ресурса ЛВС в течение одного дня сообщить об этом Администратору ЛВС.

3.3. Пользователю запрещается:

3.3.1. Блокировать доступ к ресурсам ЛВС и совершать иные действия, препятствующие штатному режиму их эксплуатации.

3.3.2. Совершать попытки несанкционированного доступа к ресурсам ЛВС, ЛВС.

3.3.3. Подключать к рабочим станциям средства беспроводной связи и средства связи с внешними информационными сетями.

3.3.4. Самовольно вносить изменения в конструкцию, конфигурацию, размещение рабочих станций и других аппаратных ресурсов ЛВС.

3.3.5. Производить установку (инсталляцию) на рабочую станцию программного обеспечения.

3.3.6. Оставлять свою рабочую станцию, подключённую к ЛВС, не выполнив выход из своей учётной записи или не осуществив ее блокировку.

3.3.7. Фиксировать свои учётные данные (пароли, идентификаторы и т.п.) для долговременного хранения на любых носителях информации (на магнитной (магнито-оптической), оптической и бумажной основе).

3.3.8. Допускать к подключённой в ЛВС рабочей станции других лиц без согласования с Администратором ЛВС.

3.3.9. Запускать на рабочей станции, подключённой к ЛВС, ПО, не входящее в состав ПО рабочей станции.

3.3.10. Устанавливать и/или использовать на рабочей станции, подключённой к ЛВС, игровое, обучающее и другое ПО, не предназначенное для исполнения служебных обязанностей.

3.3.11. Работать с неучтёнными носителями информации на магнитной (магнито-оптической) и оптической основе.

3.3.12. Производить копирование информации на неучтённые носители информации (в том числе и для временного хранения информации).

4. Порядок эксплуатации ЛВС

4.1. Администрирование и техническое обслуживание (сопровождение) телекоммуникационной инфраструктуры ЛВС осуществляются Администратором ЛВС и (или) под его непосредственным контролем.

4.2. Локальный администратор назначается заместителем Председателя Правительства Ульяновской области - Министром агропромышленного комплекса и развития сельских территорий Ульяновской области по согласованию с Оператором ЛВС.

4.3. Подключение устройств доступа в сети общего пользования осуществляется Администратором ЛВС или Локальным администратором по согласованию с Оператором ЛВС.

4.4. Настройка операционной системы рабочих станций Пользователей, установка (обновление) программных продуктов производятся Локальными администраторами.

Самостоятельная установка (обновление) программных продуктов Пользователями или посторонними лицами запрещена.

4.5. Оператор ЛВС вправе производить отключение от ЛВС любых Пользователей и ресурсов в случаях, когда они препятствуют нормальному функционированию ЛВС либо представляют угрозу безопасности информации, содержащейся в информационных ресурсах, используемых ЛВС, с последующим уведомлением руководителя структурного подразделения Министерства или подведомственной организации, в пользовании которого находятся рабочие станции, отключённые от ЛВС.

4.6. Плановое отключение ресурсов ЛВС для технологических целей может производиться только оператором ЛВС с обязательным предварительным уведомлением структурных подразделений Министерства и подведомственной организации.

4.7. Реализацию внедрения в работу ЛВС антивирусного программного обеспечения решает Администратор ЛВС. Принцип полноты охвата системой антивирусной защиты локальной сети предусматривает постепенной внедрение в сеть программных средств антивирусной защиты до полного насыщения в сочетании с организационно-режимными мерами защиты информации.

4.8. Аутентификация Пользователей в ЛВС происходит по паролю, который содержит не менее 6 символов и цифр, либо при наличии ключа безопасности на компьютерах, где происходит обработка персональных данных, при наличии такого технического средства. Пароль для аутентификации пользователя создается Администратором ЛВС, он же является Администратором информационной безопасности информационных систем Министерства.

4.9. В ЛВС отсутствует свой почтовый сервис. Пользователи, использующие в ЛВС работу с внешней электронной почтой (yandex, mail и т.д.) полностью берут на себя ответственность за сохранность пересылаемой ими информации.

5. Порядок предоставления доступа к ЛВС

5.1. Администратором ЛВС является отдел информационных технологий и защиты информации Агентства (далее – отдел защиты информации).

5.2. Действие настоящего раздела не распространяется:

5.2.1. На деятельность, связанную с обеспечением Пользователей материальными ценностями, в том числе аппаратными ресурсами.

5.2.2. На восстановление доступа Пользователям к ресурсам ЛВС, ЛВС в случае, если потеря доступа произошла в результате какой-либо технической неполадки. В случае потери пользователем доступа необходимо обращаться в отдел защиты информации.

5.3. Доступ к ресурсам ЛВС, ЛВС Пользователю предоставляется:

5.3.1. В целях обеспечения надлежащих организационно-технических условий, необходимых для исполнения своих должностных обязанностей.

5.3.2. В целях поставки товаров, выполнения работ, оказания услуг в ходе реализации государственных контрактов (договоров), связанных с функционированием ЛВС.

5.4. Доступ к информационным и программным ресурсам ЛВС осуществляется при соблюдении всех следующих условий:

5.4.1. Наличие доступа пользователей к аппаратным ресурсам (наличие автоматизированного рабочего места - рабочей станции).

5.4.2. Наличие на рабочей станции Пользователя лицензионной операционной системы, лицензионного прикладного программного обеспечения и лицензионных средств антивирусной защиты, совместимых со средствами управления, установленными на серверном оборудовании Министерства.

5.4.3. Наличие доступа Пользователей к необходимым сопутствующим ресурсам ЛВС.

5.5. Для рассмотрения вопроса о предоставлении сотруднику доступа к ЛВС и подготовке рабочей станции к эксплуатации его непосредственным руководителем оформляется заявка по форме согласно приложению № 1.

5.6. Для рассмотрения вопроса о предоставлении сотруднику Министерства или подведомственной организации доступа к ресурсам ЛВС его непосредственный руководитель оформляет заявку по форме согласно приложению № 2.

5.7. Оформленные заявки направляются в отдел защиты информации.

5.8. Отдел защиты информации в течение одного рабочего дня со дня получения заявки обеспечивает её рассмотрение в части вопросов обеспечения информационной безопасности. В случае если доступ к ресурсам ЛВС, ЛВС

не может быть предоставлен, заявка возвращается её исполнителю с указанием причины отказа в предоставлении доступа к ресурсам ЛВС, ЛВС.

5.9. В случае согласования заявки отдел защиты информации организует работу по предоставлению доступа к ресурсам ЛВС, ЛВС.

В случае отсутствия технической возможности выполнения заявки отделом защиты информации отклоненная заявка возвращается её исполнителю с указанием причины отказа в предоставлении доступа к ресурсам ЛВС, ЛВС.

Срок хранения заявок - 2 года со дня их согласования.

5.10. Информация о поступивших заявках заносится в журнал регистрации и учёта заявок на предоставление доступа к ресурсам ЛВС, ЛВС (далее - журнал регистрации заявок) по форме согласно приложению № 3, который ведётся в бумажном и (или) электронном виде отделом защиты информации.

5.11. Пользователи допускаются к работе с ресурсами ЛВС, ЛВС только после прохождения инструктажа, проводимого отделом защиты информации. Форма журнала учёта инструктажей по правилам доступа к ресурсам ЛВС, ЛВС (далее - журнал учёта инструктажей) приведена в приложении № 4.

Срок хранения журнала учёта инструктажей составляет 2 года.

5.12. Для доступа исполнителей работ (услуг), связанных с функционированием ЛВС, руководителем структурного подразделения, инициировавшего проведение данных работ (услуг), оформляется заявка по форме согласно приложению № 1.

5.13. Деятельность Пользователей, связанная с использованием ресурсов ЛВС, протоколируется, проверяется на предмет соблюдения настоящего раздела отделом защиты информации.

5.14. Информация о новом ресурсе ЛВС (изменениях в имеющемся ресурсе) должна быть доведена владельцем ресурса до отдела защиты информации в течение 2 рабочих дней с момента его появления в виде заявки по форме согласно приложению № 5. Сведения об окончании действия ресурса представляются аналогично.

5.15. Основаниями аннулирования доступа к ресурсам ЛВС, ЛВС являются:

5.15.1. Изменение должностных обязанностей сотрудника;

5.15.2. Истечение периода действия доступа;

5.15.3. Изменение технологических процессов обработки информации таким образом, что доступ к ресурсам пользователю больше не требуется;

5.15.4. Неисполнение сотрудником требований настоящего раздела;

5.15.5. Предоставление сотруднику отпуска по уходу за ребенком;

5.15.6. Прекращение служебного контракта (трудового договора) с сотрудником.

5.16. Аннулирование доступа инициируется в течение 2 рабочих дней с даты возникновения основания, предусмотренного пунктом 5.15 настоящего раздела.

5.22. Инициирование аннулирования доступа пользователя к ресурсам ЛВС осуществляют:

5.22.1. По основаниям, предусмотренным подпунктами 5.15.1, 5.15.3, 5.15.5, 5.15.6 пункта 5.16 настоящего раздела, - непосредственный руководитель сотрудника, по согласованию с отделом защиты информации.

5.22.2. По основаниям, предусмотренным подпунктами 5.15.2, 5.15.4 пункта 5.15 настоящего раздела, - отдел защиты информации.

5.23. Аннулирование доступа пользователя к ресурсам ЛВС, ЛВС осуществляется управлением аппаратного и программного обеспечения и (или) отделом защиты информации после получения заявки по форме согласно приложению № 2.

5.24. Информация об аннулировании доступа пользователя к ресурсам ЛВС, ЛВС (с указанием причины аннулирования) доводится в письменном виде отделом защиты информации до непосредственного руководителя сотрудника одновременно с инициацией данной процедуры.

5.25. Информация об аннулировании доступа пользователя к ресурсам ЛВС, ЛВС в течение одного рабочего дня со дня аннулирования заносится отделом защиты информации в журнал регистрации заявок.

5.26. Замена рабочей станции ЛВС осуществляется по инициативе Оператора ЛВС или Пользователя ЛВС.

5.27. При замене, списании и другом отчуждении рабочей станции ЛВС сотрудником по согласованию с его непосредственным руководителем оформляется заявка на гарантированное и безвозвратное удаление информации по форме согласно приложению № 6.

Срок хранения заявок - 2 года со дня их согласования.

5.28. Для рассмотрения вопроса о ремонте или тестировании средств вычислительной техники, входящих в состав ЛВС, руководителем структурного подразделения Министерства или подведомственной организации оформляется заявка по форме согласно приложению № 7.

5.29. Управление аппаратного и программного обеспечения в течение одного рабочего дня со дня получения заявки обеспечивает её рассмотрение. В случае, если ремонт или тестирование средств вычислительной техники не могут быть осуществлены, заявка возвращается ее автору с указанием причины отказа.

Срок хранения заявок - 2 года со дня их согласования.

5.30. Контроль за соблюдением настоящего раздела осуществляется отделом защиты информации.

6. Актуализация информации о Пользователях ЛВС

Для актуализации информации о Пользователях ЛВС руководители структурных подразделений Министерства или подведомственной организации с периодичностью не реже 1 раза в месяц направляют Оператору ЛВС перечень принятых и уволенных сотрудников, являющихся Пользователями ЛВС.

7. Обработка информации ограниченного доступа

7.1. Для обработки информации ограниченного доступа Оператором ЛВС могут создаваться ЗЛВС.

7.1.1. Требования к ЗЛВС определяются Оператором ЛВС и согласуются с отделом защиты информации.

7.1.2. ЗЛВС должны соответствовать требованиям руководящих документов Федеральной службы по техническому и экспортному контролю Российской Федерации и Федеральной службы безопасности Российской Федерации.

7.1.3. Перечень организационно-распорядительной документации, устанавливающей порядок администрирования и работы в ЗЛВС, определяется оператором ЛВС и отделом защиты информации.

7.2. Пользователям ЛВС запрещается использование открытого сегмента ЛВС для обработки, хранения и передачи информации ограниченного доступа.

8. Действия при нарушении режима функционирования ЛВС

8.1. Реакция на нарушения режима функционирования ЛВС преследует две главные цели:

8.1.1. Блокирование источника нарушения и уменьшение наносимого вреда.

8.1.2. Недопущение повторных нарушений.

8.2 Функции по выявлению нарушений и оперативное реагирование на них осуществляет оператор ЛВС, локальные администраторы и пользователи ЛВС.

8.3. Восстановительные работы в ЛВС производятся оператором ЛВС в соответствии с Планом восстановительных работ, утверждаемым оператором ЛВС.

8.4. Основными принципами проведения восстановительных работ являются:

обеспечение максимальной сохранности информационных ресурсов ЛВС;

поддержание остаточной работоспособности и доступности максимального количества ресурсов сети пользователям;

минимизация времени восстановительных работ.

8.5. Перед проведением работ пользователи ЛВС должны быть оповещены о предполагаемой продолжительности работ и связанных с ними ограничениях.

9. Ответственность за нарушение порядка работы с ЛВС

9.1. Ответственность за нарушение порядка информационного обмена в ЛВС и передачи информации за её пределы несёт руководитель структурного

подразделения - Пользователя ЛВС, в которой данная информация обрабатывается.

9.2. Каждый Пользователь ЛВС несёт персональную ответственность за нарушение настоящего Положения обработки информации на своем рабочем месте.

В случае несанкционированного доступа к информации на рабочих станциях, наличия вредоносного программного обеспечения и нарушения правил, установленных настоящим Положением, рабочая станция отключается от ЛВС с уведомлением руководителя соответствующего структурного подразделения.

Приложение № 1
к Положению об использовании
локальной вычислительной сети
в Министерстве агропромышленного
комплекса и развития сельских
территорий Ульяновской области
и подведомственной ему организации

Начальнику отдела
информационных технологий
и защиты информации

_____
(ФИО)

ЗАЯВКА
о предоставлении доступа к ЛВС

Прошу Вас рассмотреть вопрос о предоставлении доступа к локальной вычислительной сети Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области, установить операционную систему и следующее программное обеспечение _____

_____

_____:

N п/п	ФИО сотрудника	Должность сотрудника	Инвентарный номер рабочей станции	Сетевое имя рабочей станции	Номер кабинета	Номер телефона	Период доступа
1	2	3	4	5	6	7	8

_____ _____
(должность руководителя (ФИО) структурного подразделения) (Подпись)

_____
Дата

Приложение № 2
к Положению об использовании
локальной вычислительной сети
в Министерстве агропромышленного
комплекса и развития сельских
территорий Ульяновской области
и подведомственной ему организации

Начальнику отдела
информационных технологий
и защиты информации

_____
(ФИО)

ЗАЯВКА
о предоставлении доступа к ресурсу ЛВС

№ п/п	ФИО пользователя, должность	Инвентарный номер рабочей станции, номер комнаты, номер телефона	Сетевое имя рабочей станции	Обоснование необходимости представления / аннулирования доступа к ресурсам локальной вычислительной сети (с указанием подпунктов должностного регламента (инструкции)	Наименование предоставляемого ресурса	Режим доступа <1>	Период действия доступа
1	2	3	4	5	6	7	8

<1> Открыть/закрыть, чтение/запись, просмотр, ввод, корректировка, возможность печати.

_____ _____
(должность руководителя (ФИО) структурного подразделения) (Подпись)

_____
Дата

Приложение № 3
к Положению об использовании
локальной вычислительной сети
в Министерстве агропромышленного
комплекса и развития сельских
территорий Ульяновской области
и подведомственной ему организации

ЖУРНАЛ
регистрации и учёта заявок
на предоставление доступа к ресурсам ЛВС, ЛВС

N п/п	Номер заявки	Наименование подразделения	Дата согласования заявки	Период доступа
1	2	3	4	5

Приложение № 4
к Положению об использовании
локальной вычислительной сети
в Министерстве агропромышленного
комплекса и развития сельских
территорий Ульяновской области
и подведомственной ему организации

ЖУРНАЛ
учёта инструктажей по правилам доступа
к ресурсам ЛВС, ЛВС

N п/п	С кем проведен инструктаж			Инструктаж провел		
	ФИО сотрудника	Должность сотрудника	Подпись	ФИО, должность	Подпись	Дата
1	2	3	4	5	6	7

Приложение № 5
к Положению об использовании
локальной вычислительной сети
в Министерстве агропромышленного
комплекса и развития сельских
территорий Ульяновской области
и подведомственной ему организации

Начальнику отдела
информационных технологий
и защиты информации

_____
(ФИО)

ЗАЯВКА
о включении нового (аннулировании)
информационного ресурса

В соответствии с Положением об использовании локальной вычислительной сети в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации прошу включить новый (аннулировать) информационный ресурс

_____
_____
_____:
(указать наименование органа, структурного подразделения - владельца ресурса)

N п/п	Наименование информационного ресурса	Основание для включения нового (аннулирования) ресурса	Период действия
1	2	3	4

_____ _____
(должность руководителя (ФИО) структурного подразделения) (Подпись)

_____
Дата

_____

Приложение № 6
к Положению об использовании
локальной вычислительной сети
в Министерстве агропромышленного
комплекса и развития сельских
территорий Ульяновской области
и подведомственной ему организации

Начальнику отдела
информационных технологий
и защиты информации

_____

(ФИО)

ЗАЯВКА
на гарантированное и безвозвратное удаление информации с рабочей станции

В соответствии с Положением об использовании локальной вычислительной сети в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации прошу произвести гарантированное и безвозвратное удаление информации с рабочей станции, инвентарный номер _____.

С последствиями производимой операции ознакомлен и согласен.

_____ _____
(должность руководителя (ФИО) структурного подразделения) (Подпись)

_____ _____
(должность сотрудника (ФИО) структурного подразделения) (Подпись)

_____
Дата

_____

Приложение № 7
к Положению об использовании
локальной вычислительной сети
в Министерстве агропромышленного
комплекса и развития сельских
территорий Ульяновской области
и подведомственной ему организации

Начальнику отдела
информационных технологий
и защиты информации

_____
(ФИО)

ЗАЯВКА
об организации ремонта и (или) тестирования средств вычислительной техники, входящих в состав ЛВС

В соответствии с Положением об использовании локальной вычислительной сети в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации прошу организовать ремонт и (или) тестирование средств вычислительной техники:

N п/п	ФИО сотрудника	Должность	Инвентарный номер	Номер кабинета	Номер телефона
1	2	3	4	5	6

_____ _____
(должность руководителя (ФИО) структурного подразделения) (Подпись)

_____
Дата

ПРИЛОЖЕНИЕ № 2

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 371

ПОРЯДОК
эксплуатации средств криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

1. Общие положения

1.1. Порядок эксплуатации средств криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (далее – Порядок) регламентирует организацию и обеспечение функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну (далее – СКЗИ, криптосредство) в случае их использования для обеспечения безопасности конфиденциальной информации и персональных данных в рамках их обработки в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и подведомственной ему организации (далее – подведомственная организация).

1.2. Настоящий Порядок разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом «О персональных данных» от 27.07.2006 № 152-ФЗ, Федеральным законом «Об электронной подписи» от 06.04.2011 № 63-ФЗ, приказом ФСБ России от 10.07.2014 № 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», приказом ФАПСИ от 13.06.2001 № 152 «Об утверждении Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом,

не содержащей сведений, составляющих государственную тайну», приказом ФСБ РФ от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения в области эксплуатации СКЗИ.

1.3. Порядок распространяется на криптосредства, предназначенные для обеспечения безопасности конфиденциальной информации и персональных данных при их обработке в информационных системах Министерства.

1.4. СКЗИ, реализующие функции шифрования и электронной подписи применяются для защиты электронных документов, передаваемых по общедоступным каналам связи.

1.5. Для обеспечения безопасности необходимо использовать СКЗИ, которые:

допускают встраивание в технологические процессы обработки электронных сообщений, обеспечивают взаимодействие с прикладным программным обеспечением на уровне обработки запросов на криптографические преобразования и выдачи результатов;

поставляются разработчиками с полным комплектом эксплуатационной документации, включая описание ключевой системы, правила работы с ней, а также обоснование необходимого организационно-штатного обеспечения;

поддерживают непрерывность процессов протоколирования работы СКЗИ и обеспечения целостности программного обеспечения для среды функционирования СКЗИ, представляющей собой совокупность технических и программных средств, совместно с которыми происходит штатное функционирование СКЗИ и которые способны повлиять на выполнение предъявляемых к СКЗИ требований;

сертифицированы уполномоченным государственным органом либо имеют разрешение ФСБ России.

1.6. СКЗИ, применяемые для защиты персональных данных, должны иметь класс не ниже КС2.

1.7. СКЗИ реализуются на основе криптографических алгоритмов, утвержденных в качестве национальных стандартов и соответствующих условиям договора с контрагентом.

1.8. СКЗИ и документация на СКЗИ приобретаются самостоятельно или могут быть получены у сторонней организации, инициирующей защищенный документооборот.

1.9. СКЗИ, включая инсталляционные носители, ключевые документы, описания и инструкции к СКЗИ, составляют коммерческую тайну.

2. Порядок применения СКЗИ

2.1. Установка и настройка СКЗИ осуществляется в соответствии с эксплуатационной документацией, инструкциями ФСБ России, других

организаций, участвующих в защищённом электронном документообороте. По окончании установки и настройки осуществляется проверка готовности СКЗИ к использованию с составлением акта установки СКЗИ согласно приложению № 1.

Размещение и монтаж СКЗИ, а также другого оборудования, функционирующего с криптосредствами, в режимных помещениях должны свести к минимуму возможность неконтролируемого доступа посторонних лиц к указанным средствам. Техническое обслуживание такого оборудования и смена криптоключей осуществляются в отсутствие лиц, не допущенных к работе с данными СКЗИ. Необходимо предусмотреть организационно-технические меры, исключающие возможность использования СКЗИ посторонними лицами. Физическое размещение СКЗИ должно обеспечивать безопасность СКЗИ, предотвращение несанкционированного доступа к СКЗИ. Доступ лиц в помещения, где располагаются СКЗИ, ограничивается в соответствии со служебной (трудовой) необходимостью и определяется утверждённым перечнем лиц, доступ которых необходим для выполнения ими служебных (трудовых) обязанностей. Встраивание криптосредств класса КС1 и КС2 осуществляется без контроля со стороны ФСБ России (если этот контроль не предусмотрен техническим заданием на разработку (модернизацию) информационной системы).

Встраивание криптосредств класса КС1 или КС2 может осуществляться либо самим пользователем криптосредства при наличии соответствующей лицензии ФСБ России, либо организацией, имеющей соответствующую лицензию ФСБ России.

Снятие СКЗИ с эксплуатации осуществляется при соблюдении процедур, обеспечивающих гарантированное удаление информации, несанкционированное использование которой может нанести ущерб деятельности Министерства и подведомственной организации, и информации, используемой средствами обеспечения информационной безопасности, из постоянной памяти и с внешних носителей (за исключением архивов электронных документов и протоколов электронного взаимодействия, ведение и сохранность которых в течение определенного срока предусмотрены соответствующими нормативными правовыми актами и (или) договорными документами) и оформляется актом уничтожения СКЗИ согласно приложению № 2. СКЗИ уничтожают по решению владельца (пользователя) криптосредства с уведомлением подразделения, ответственного за организацию поэкземплярного учёта криптосредств.

Намеченные к уничтожению СКЗИ подлежат изъятию из аппаратных средств, с которыми они функционировали. При этом криптосредства считаются изъятыми из аппаратных средств, если исполнена предусмотренная эксплуатационной и технической документацией к СКЗИ процедура удаления программного обеспечения криптосредств, и они полностью отсоединены от аппаратных средств.

Пригодные для дальнейшего использования узлы и детали аппаратных средств общего назначения, не предназначенные специально для аппаратной

реализации криптографических алгоритмов или иных функций СКЗИ, а также совместно работающее с криптосредствами оборудование (мониторы, принтеры, сканеры, клавиатура и т.п.), разрешается использовать после уничтожения СКЗИ без ограничений. При этом информация, которая может оставаться в устройствах памяти оборудования (например, в принтерах, сканерах), должна быть надежно удалена (стерта).

2.2. Эксплуатация СКЗИ осуществляется лицами, назначенными распоряжением Министерства и прошедшими обучение по работе с криптосредствами. При наличии двух и более пользователей СКЗИ обязанности между ними распределяются с учётом персональной ответственности за сохранность криптосредств, ключевой, эксплуатационной и технической документации, а также за порученные участки работы (Приложение № 3, Приложение № 4).

Пользователи криптосредств обязаны:

не разглашать информацию, к которой они допущены, в том числе сведения о СКЗИ и других мерах защиты;

не разглашать информацию о ключевых документах;

не допускать снятие копий с ключевых документов;

не допускать вывод ключевых документов на дисплей (монитор) персональной электронно-вычислительной машины или принтер;

не допускать записи на ключевой носитель посторонней информации;

не допускать установки ключевых документов в другие персональные электронно-вычислительные машины;

соблюдать требования к обеспечению безопасности информации, требования к обеспечению безопасности СКЗИ и ключевых документов к ним;

сообщать о ставших им известными попытках несанкционированного доступа к сведениям об используемых СКЗИ или ключевых документах к ним;

немедленно уведомлять о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей от помещений, хранилищ, личных печатей и о других фактах, которые могут привести к разглашению защищаемой информации;

сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы при увольнении или отстранении от исполнения обязанностей, связанных с использованием криптосредств.

Безопасность обработки информации с использованием СКЗИ обеспечивается:

соблюдением ответственными лицами, допущенными к работе с СКЗИ, конфиденциальности при обращении со сведениями, которые им доверены или стали известны по работе, в том числе со сведениями о функционировании и порядке обеспечения безопасности применяемых СКЗИ и ключевых документах к ним;

точным выполнением пользователями СКЗИ требований к обеспечению безопасности информации;

надежным хранением эксплуатационной и технической документации к СКЗИ, ключевых документов, носителей информации ограниченного распространения;

своевременным выявлением попыток несанкционированного доступа к сведениям о защищаемой информации, об используемых СКЗИ или ключевых документах к ним;

немедленным принятием мер по предупреждению разглашения защищаемой информации, а также возможной её утечки при выявлении фактов утраты или недостачи СКЗИ, ключевых документов к ним, удостоверений, пропусков, ключей от помещений, хранилищ, сейфов (металлических шкафов), личных печатей и т.п.

При необходимости передачи по техническим средствам связи служебных сообщений ограниченного доступа, касающихся организации и обеспечения функционирования СКЗИ, указанные сообщения необходимо передавать только с использованием криптосредств. Передача по техническим средствам связи криптоключей не допускается, за исключением специально организованных систем с децентрализованным снабжением криптоключами.

Используемые или хранимые СКЗИ, эксплуатационная и техническая документация к ним, ключевые документы подлежат поэкземплярному учёту в журнале учёта СКЗИ согласно приложению № 5 и приложению № 6. При этом программные СКЗИ должны учитываться совместно с аппаратными средствами, с которыми осуществляется их штатное функционирование. Если аппаратные или аппаратно-программные СКЗИ подключаются к системной шине или к одному из внутренних интерфейсов аппаратных средств, то такие криптосредства учитываются также совместно с соответствующими аппаратными средствами.

Единицей поэкземплярного учёта ключевых документов считается ключевой носитель многократного использования, ключевой блокнот. Если один и тот же ключевой носитель многократно используют для записи криптоключей, то его каждый раз следует регистрировать отдельно.

Все полученные экземпляры криптосредств, эксплуатационной и технической документации к ним, ключевых документов должны быть выданы под расписку в соответствующем журнале поэкземплярного учёта лиц, допущенных к работе с СКЗИ, несущим персональную ответственность за их сохранность.

Администратор информационной безопасности информационных систем Министерства (далее – Администратор ИБ ИС Министерства) заводит и ведёт на каждого пользователя СКЗИ (каждое структурное подразделение, кому передаётся СКЗИ) лицевой счёт по форме согласно приложению № 7, в котором регистрирует числящиеся за ними СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы.

Передача СКЗИ, эксплуатационной и технической документации к ним, ключевых документов допускается только между работниками криптосредств и (или) ответственным работником криптосредств под

расписку в соответствующих журналах поэкземплярного учёта. Такая передача между работниками криптосредств должна быть санкционирована.

Хранение инсталлирующих носителей СКЗИ, эксплуатационной и технической документации, ключевых документов осуществляется в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их непреднамеренное уничтожение.

Аппаратные средства, с которыми осуществляется штатное функционирование СКЗИ, а также аппаратные и аппаратно-программные СКЗИ должны быть оборудованы средствами контроля за их вскрытием. Место опечатывания (опломбирования) криптосредств, аппаратных средств должно быть таким, чтобы его можно было визуально контролировать. При наличии технической возможности на время отсутствия работников криптосредства необходимо отключать от линии связи и убирать в опечатываемые места.

Внесение изменений в программное обеспечение СКЗИ и техническую документацию на СКЗИ осуществляется на основании полученных от производителя СКЗИ и документально подтвержденных обновлений с фиксацией контрольных сумм.

Эксплуатация СКЗИ предполагает ведение не менее двух резервных копий программного обеспечения и одной резервной копии ключевых носителей. Восстановление работоспособности СКЗИ в аварийных ситуациях осуществляется в соответствии с эксплуатационной документацией.

2.3. Изготовление ключевых документов из исходной ключевой информации осуществляют ответственные пользователи СКЗИ, применяя штатные криптосредства, если такая возможность предусмотрена эксплуатационной и технической документацией при наличии полученной лицензии ФСБ России на деятельность по изготовлению ключевых документов для криптосредств.

Ключевые документы могут доставляться фельдъегерской (в том числе ведомственной) связью или со специально выделенными ответственными пользователями криптосредств и работниками Министерства или подведомственной организации при соблюдении мер, исключающих бесконтрольный доступ к ключевым документам во время доставки.

Для пересылки ключевых документов они должны быть помещены в прочную упаковку, исключающую возможность их физического повреждения и внешнего воздействия. На упаковках указывают ответственного лица, допущенного к работе с СКЗИ, для которого эти упаковки предназначены. На таких упаковках делают пометку «Лично». Упаковки опечатывают таким образом, чтобы исключалась возможность извлечения из них содержимого без нарушения упаковок и оттисков печати.

До первоначальной высылки (или возвращения) адресату сообщают отдельным письмом описание высылаемых ему упаковок и печатей, которыми они могут быть опечатаны.

Для пересылки ключевых документов готовится сопроводительное письмо, в котором необходимо указывается: что посылается и в каком количестве, учётные номера документов, а также, при необходимости, назначение и порядок использования высылаемого отправления. Сопроводительное письмо вкладывают в одну из упаковок.

Полученные упаковки вскрывает только ответственное лицо, допущенное к работе с СКЗИ, для которых они предназначены. Если содержимое полученной упаковки не соответствует указанному в сопроводительном письме или сама упаковка и печать - их описанию (оттиску), а также если упаковка повреждена, в результате чего образовался свободный доступ к её содержимому, то лицо, допущенное к работе с СКЗИ, составляет акт, который высылает отправителю. Полученные с такими отправлениями ключевые документы до получения указаний от отправителя применять не разрешается.

При обнаружении бракованных ключевых документов или криптоключей один экземпляр бракованного изделия следует возвратить изготовителю для установления причин происшедшего и их устранения в дальнейшем, а оставшиеся экземпляры хранить до поступления дополнительных указаний от изготовителя.

Получение ключевых документов должно быть подтверждено отправителю в соответствии с порядком, указанным в сопроводительном письме. Отправитель обязан контролировать доставку своих отправлений адресатам. Если от адресата своевременно не поступило соответствующего подтверждения, то отправитель должен направить ему запрос и принять меры к уточнению местонахождения отправлений.

Заказ на изготовление очередных ключевых документов, их изготовление и рассылку на места использования для своевременной замены действующих ключевых документов производится заблаговременно. Указание о вводе в действие очередных ключевых документов дается ответственным лицом, допущенных к работе с СКЗИ, только после поступления от них подтверждения о получении очередных ключевых документов.

Неиспользованные или выведенные из действия ключевые документы подлежат возвращению или должны быть уничтожены. Уничтожение криптоключей (исходной ключевой информации) может производиться путём физического уничтожения ключевого носителя, на котором они расположены, или путём стирания (разрушения) криптоключей (исходной ключевой информации) без повреждения ключевого носителя (для обеспечения возможности его многократного использования). Криптоключи (исходную ключевую информацию) стирают по технологии, принятой для соответствующих ключевых носителей многократного использования (дискет, компакт-дисков (CD-ROM), Rutoken, Data Key, Smart Card, Touch Memory и т.п.). Непосредственные действия по стиранию криптоключей (исходной ключевой информации), а также возможные ограничения на дальнейшее применение соответствующих ключевых

носителей многократного использования регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Ключевые носители уничтожают путём нанесения им неустранимого физического повреждения, исключающего возможность их использования, а также восстановления ключевой информации. Непосредственные действия по уничтожению конкретного типа ключевого носителя регламентируются эксплуатационной и технической документацией к соответствующим СКЗИ, а также указаниями организации, производившей запись криптоключей (исходной ключевой информации).

Бумажные и прочие сгораемые ключевые носители уничтожают путём сжигания или с помощью любых бумагорезательных машин.

Ключевые документы уничтожаются в сроки, указанные в эксплуатационной и технической документации к соответствующим СКЗИ. Факт уничтожения оформляется в соответствующих журналах поэкземплярного учёта.

Уничтожение производит комиссия в составе не менее двух человек. В акте указывается, что уничтожается и в каком количестве. В конце акта делается итоговая запись (цифрами и прописью) о количестве наименований и экземпляров уничтожаемых ключевых документов, инсталлирующих СКЗИ носителей, эксплуатационной и технической документации. Исправления в тексте акта должны быть оговорены и заверены подписями всех членов комиссии, принимавших участие в уничтожении. О проведённом уничтожении делаются отметки в соответствующих журналах поэкземплярного учёта.

Криптоключи, в отношении которых возникло подозрение в компрометации, а также действующие совместно с ними другие криптоключи необходимо немедленно вывести из действия, если иной порядок не оговорён в эксплуатационной и технической документации СКЗИ. В чрезвычайных случаях, когда отсутствуют криптоключи для замены скомпрометированных, допускается по решению ответственного пользователя криптосредств использование скомпрометированных криптоключей. В этом случае период использования скомпрометированных криптоключей должен быть максимально коротким, а защищаемая информация как можно менее ценной.

О нарушениях, которые могут привести к компрометации криптоключей, их составных частей или передававшихся (хранящихся) с их использованием данных, пользователи криптосредств обязаны сообщать Администратору ИБ ИС Министерства.

Осмотр ключевых носителей многократного использования посторонними лицами не следует рассматривать, как подозрение в компрометации криптоключей, если при этом исключалась возможность их копирования (чтения, размножения).

В случаях недостачи, не предъявления ключевых документов, а также неопределенности их местонахождения ответственный пользователь, допущенный к работе с СКЗИ, принимает срочные меры к их розыску и локализации последствий компрометации ключевых документов.

3. Порядок управления ключевой системой

3.1. Регистрация лиц, обладающих правами по управлению ключами, осуществляется в соответствии с эксплуатационной документацией на СКЗИ.

3.2. Управление ключами – информационный процесс, включающий в себя три элемента:

генерацию ключей;

накопление ключей;

распределение ключей.

3.3. В информационных системах Министерства используются специальные аппаратные и программные методы генерации случайных ключей. Как правило, используются датчики псевдослучайных чисел (далее ПСЧ), с достаточно высокой степенью случайности их генерации. Вполне приемлемы программные генераторы ключей, которые вычисляют ПСЧ, как сложную функцию от текущего времени и (или) числа, введённого лицом.

3.4. Под накоплением ключей понимается организация их хранения, учёта и удаления.

Секретные ключи не должны записываться в явном виде на носителе, который может быть считан или скопирован.

Вся информация об используемых ключах должна храниться в зашифрованном виде. Ключи, зашифровывающие ключевую информацию, называются мастер-ключами. Мастер-ключи каждый пользователь должен знать наизусть, запрещается хранение их на каких-либо материальных носителях.

Для условия безопасности информации необходимо периодическое обновление ключевой информации в информационных системах Министерства. При этом переназначаются как обычные ключи, так и мастер-ключи.

3.5. При распределении ключей необходимо выполнить следующие требования:

оперативность и точность распределения;

скрытость распределяемых ключей.

3.6. Управление ключами, основанное на системах с открытым ключом.

До использования криптосистемы с открытым ключом для обмена обычными секретными ключами пользователи должны обменяться своими открытыми ключами.

Управление открытыми ключами может быть организовано с помощью оперативной или автономной службы каталогов, пользователи могут также обмениваться ключами непосредственно.

4. Мониторинг и контроль применения СКЗИ

4.1. Для повышения уровня безопасности при эксплуатации СКЗИ в автоматизированной системе следует реализовать процедуры мониторинга, регистрирующие все значимые события, состоявшиеся в процессе обмена электронными сообщениями, и все инциденты информационной безопасности. Описание и перечень данных процедур должны быть установлены в эксплуатационной документации на СКЗИ.

4.2. Контроль применения СКЗИ обеспечивает:

контроль соответствия настройки и конфигурирования средств защиты информации, а также технических и программных средств, способных повлиять на выполнение предъявляемых к средствам защиты информации требований, нормативной и технической документации;

контроль соблюдения правил хранения информации ограниченного доступа, используемой при эксплуатации средств защиты информации (в частности, ключевой, парольной и аутентифицирующей информации);

контроль возможности доступа посторонних лиц к средствам защиты информации, а также к техническим и программным средствам, способным повлиять на выполнение предъявляемых к средствам защиты информации требований;

контроль соблюдения правил реагирования на инциденты информационной информации (о фактах утраты, компрометации ключевой, парольной и аутентифицирующей информации, а также любой другой информации ограниченного доступа);

контроль соответствия технических и программных средств СКЗИ и документации на эти средства эталонным образцам (гарантии поставщиков или механизмы контроля, позволяющие установить самостоятельно такое соответствие);

контроль целостности технических и программных средств СКЗИ и документации на эти средства в процессе хранения и ввода в эксплуатацию этих средств (с использованием как механизмов контроля, описанных в документации на СКЗИ).

ПРИЛОЖЕНИЕ № 1
к Порядку эксплуатации средств криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

АКТ
установки средств криптографической защиты информации (СКЗИ)

«____» _____ 20___

Настоящий акт составлен о том, что комиссия_____
Указывается наименование организации

в составе:

_____
ФИО, должность членов комиссии

произвела установку и настройку СКЗИ _____
Наименование

Серийный № (Инв. №) автоматизированного рабочего места (далее - АРМ)

_____

_____
Адрес местонахождения, номер помещения

ФИО, должность пользователя АРМ (заявитель): _____

_____

Рег. № дистрибутива СКЗИ (номер экземпляра) _____
Номер и дата карточки учета лицензии _____

Размещение АРМ заявителя, хранение ключевых носителей, охрана помещений организованы установленным порядком.
Обучение правилам работы с СКЗИ и проверка знаний нормативных правовых актов и эксплуатационной и технической документации к нему проведены.
Условия для использования СКЗИ, установленные эксплуатационной и технической документацией к СКЗИ созданы.
Установленное и настроенное СКЗИ находится в работоспособном состоянии.
Формуляр передан на ответственное хранение пользователю АРМ заявителя.
Пользователь АРМ (заявитель) обязуется:

1) не разглашать конфиденциальную информацию, к которой он допущен, в том числе криптоключи и сведения о ключевой информации;

2) соблюдать требования к обеспечению безопасности СКЗИ и ключевых документов к нему;
3) сдать установочный комплект СКЗИ, эксплуатационную и техническую документацию к нему, ключевые документы при увольнении или отстранения от исполнения обязанностей, связанных с использованием СКЗИ;
4) сообщать исполнителю о попытках посторонних лиц получить сведения об используемом СКЗИ или ключевых документах к нему;
5) немедленно уведомлять исполнителя о фактах утраты или недостачи СКЗИ, ключевых документов к нему.

Акт составлен в двух экземплярах на 1 листе каждый.
Подписи членов комиссии:

_____

_____

ФИО членов комиссии / подпись

_____

ПРИЛОЖЕНИЕ № 2
к Порядку эксплуатации средств криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

АКТ
уничтожения средств криптографической защиты информации (СКЗИ)

«____» _____ 20___

Комиссия_____
Указывается наименование организации

в составе: _____
ФИО, должность членов комиссии

составила настоящий акт о том, что на системном блоке с серийным (инвентарным) номером №_____ произведено уничтожение _____
Наименование СКЗИ

серийный № дистрибутива (№ экземпляра) _____, путем удаления программ через «Панель управления» - «Установка и удаление программ» и утилиту очистки компьютера от не удаленных элементов продуктов _____
Наименование утилиты

Диск с дистрибутивом, документация, карточка учета лицензии СКЗИ _____
Наименование СКЗИ

версии_____ от _____№ ____ подготовлена к возврату в
Версия СКЗИ

_____.
Указать уполномоченный орган

Настоящий акт составлен в 2-х экземплярах на 1 листе каждый.

Подписи членов комиссии:

_____

_____
ФИО членов комиссии / подпись

_____

ПРИЛОЖЕНИЕ № 3
к Порядку эксплуатации средств криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

ЖУРНАЛ
учёта лиц, допущенных к работе со средствами криптографической защиты информации (СКЗИ)

№ п/п	ФИО и должность допущенного к работе с СКЗИ	Наименование СКЗИ	Серийный номер СКЗИ
1	2	3	4

ПРИЛОЖЕНИЕ № 4
к Порядку эксплуатации средств
криптографической защиты
информации в Министерстве
агропромышленного комплекса
и развития сельских территорий
Ульяновской области и
подведомственной ему организации

ЗАКЛЮЧЕНИЕ
о допуске пользователя средств криптографической защиты информации (СКЗИ) к самостоятельной работе

Пользователь СКЗИ _____
ФИО сотрудника

_____
Должность

в соответствии с Инструкцией об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утвержденной Приказом ФАПСИ от 13.06.2001 № 152 при использовании СКЗИ

_____
Наименование СКЗИ

обязуется:

1) не разглашать конфиденциальную информацию, к которой допущен, рубежи её защиты, в том числе, сведения о криптоключах;

2) соблюдать требования к обеспечению безопасности конфиденциальной информации с использованием СКЗИ;

3) сообщать в орган криптографической защиты о ставших ему известными попытках посторонних лиц получить сведения об используемых СКЗИ или ключевых документах к ним;

4) сдать СКЗИ, эксплуатационную и техническую документацию к ним, ключевые документы в соответствии с установленным порядком при увольнении или отстранении от обязанностей, связанных с использованием СКЗИ;

5) немедленно уведомлять орган криптографической защиты о фактах утраты или недостачи СКЗИ, ключевых документов к ним, ключей

от помещений, хранилищ (сейфов), личных печатей и о других фактах, которые могут привести к разглашению защищаемых сведений конфиденциального характера, а также о причинах и условиях возможной утечки таких сведений.

Заключение: к самостоятельной работе с СКЗИ_____
_____допущен.
Наименование СКЗИ

С заключением ознакомлен (а): _____ _____
Подпись ФИО

Администратор информационной безопасности информационных систем Министерства _____ _____
Подпись ФИО

_____

ПРИЛОЖЕНИЕ № 5
к Порядку эксплуатации средств
криптографической защиты информации
в Министерстве агропромышленного комплекса
и развития сельских территорий Ульяновской
области и подведомственной ему организации

ЖУРНАЛ
учёта средств криптографической защиты информации (СКЗИ)

№ п.п.	Наименование криптосредства, эксплуатационной и технической документации к ним, ключевых документов	Регистрационные номера СКЗИ, эксплуатационной и технической документации к ним	Отметка о получении		Отметка о выдаче		Отметка о подключении (установке) СКЗИ			Отметка об изъятии СКЗИ из аппаратных средств, уничтожении ключевых документов			Приме-чание
			От кого получены	Дата и номер сопроводительного документа	Подпись, ФИО пользователя	Дата	Подпись, ФИО пользователя криптосредств, производившего подключение (установку)	Дата подключения (установки) и подписи лиц, произведших подключение (установку)	Номера аппаратных средств, в которые установлены или к которым подключены криптосредства	Дата изъятия (уничтожения)	Подпись, ФИО пользователя СКЗИ, производившего изъятие (уничтожение)	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10	11	12	13	14

ПРИЛОЖЕНИЕ № 6
к Порядку эксплуатации средств
криптографической защиты информации
в Министерстве агропромышленного
комплекса и развития сельских территорий
Ульяновской области и подведомственной
ему организации

ЖУРНАЛ
учёта ключевых носителей

№ п/п	Наименование ключевых документов	Номера серий ключевых документов	Номера экземпляров (криптографические номера) ключевых документов	Отметка о выдаче		Отметка об уничтожении ключевых документов			Приме-чание
				Подпись, ФИО пользователя	Дата	Дата	Подпись, ФИО пользователя СКЗИ, производившего уничтожение	Номер акта или расписка об уничтожении	
1	2	3	4	5	6	7	8	9	10

ПРИЛОЖЕНИЕ № 7
к Порядку эксплуатации средств
криптографической защиты информации
в Министерстве агропромышленного
комплекса и развития сельских территорий
Ульяновской области и подведомственной
ему организации

Книга лицевых счетов пользователей средств криптографической защиты информации (СКЗИ)

Опись лицевых счетов

№ п/п	ФИО	№ по картотеке	Расписка лица, оформившего л/с
1	2	3	4

ЛИЦЕВОЙ СЧЁТ №___

Пользователь СКЗИ:

ФИО, должность

Наименование СКЗИ	Серийные номера СКЗИ	Регистрационные номера экземпляров ключевых документов	Дата и номер подтверждения или расписка о получении СКЗИ	Дата и номер подтверждения или расписка о возвращении / уничтожении СКЗИ	Примечания
1	2	3	4	5	6

ПРИЛОЖЕНИЕ № 3

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 371

ПОРЯДОК
доступа в помещения, где размещены используемые Министерством агропромышленного комплекса и развития сельских территорий Ульяновской области и его подведомственной организацией средства криптографической защиты информации

1. Порядок доступа в помещения, где размещены используемые Министерством агропромышленного комплекса и развития сельских территорий Ульяновской области и его подведомственной организацией средства криптографической защиты информации (далее - Порядок) разработан в целях организации режима обеспечения безопасности помещений, в которых размещены используемые Министерством агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и его подведомственной организацией (далее – подведомственная организация) средства криптографической защиты информации (далее – СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ информационных систем Министерства в рабочее и нерабочее время, а также в нештатных ситуациях.

2. Помещения оснащаются входными дверьми с замками, обеспечения постоянного закрытия дверей помещений на замок и их открытия только для санкционированного прохода, а также опечатывания помещений по окончании рабочего дня или оборудование помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном вскрытии помещений.

3. Помещения располагаются в пределах контролируемой зоны, границами которой являются ограждающие конструкции здания по адресу Ульяновская обл., г. Ульяновск, ул. Радищева, д. 5.

4. Доступ в помещения в рабочее (служебное) время имеют сотрудники, включенные в перечень ответственных лиц, имеющих доступ в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, в рабочее и нерабочее время, а также в нештатных ситуациях.

5. Нахождение в помещениях посторонних лиц, без наличия в них ответственных специалистов в рабочее (служебное) и нерабочее (неслужебное) время запрещается. Лица, не имеющие право доступа в служебные помещения, допускаются в такие помещения в присутствии ответственных лиц, имеющих

право доступа в служебные помещения. Время нахождения в помещениях ограничивается временем решения вопросов, в рамках которого возникла необходимость пребывания в помещении.

6. Вскрытие и закрытие (опечатывание) служебных помещений, производится ответственными лицами, имеющими право доступа в данные помещения.

7. В рабочее (служебное) время ответственные лица, имеющие право доступа в служебные помещения не должны оставлять в отсутствие лиц, имеющих право доступа в помещение, незапертым служебное помещение.

8. Перед открытием помещений, ответственные лица, имеющие право доступа в помещения, обязаны провести внешний осмотр с целью установления целостности двери и замка, открыть дверь и осмотреть помещение, проверить наличие и целостность имеющихся печатей (пломб).

9. При обнаружении неисправности двери и запирающих устройств ответственные лица, имеющие право доступа в помещения, обязаны:

не вскрывая помещение, доложить непосредственному руководителю;

в присутствии не менее двух иных работников, включая непосредственного руководителя, вскрыть помещение и осмотреть его;

составить акт о выявленных нарушениях и передать его руководителю для служебного расследования.

10. В нештатных ситуациях, в случае необходимости принятия в рабочее (служебное) время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, иных аналогичных случаях действия работников осуществляются в соответствии с установленными правилами пожарной безопасности и иными правилами обеспечения безопасности жизнедеятельности. При этом по возможности работниками, осуществляющими работу в данном помещении, организуется контроль допуска в данные помещения обслуживающего или иного персонала.

11. В нештатных ситуациях, в случае необходимости принятия в нерабочее время экстренных мер при срабатывании пожарной или охранной сигнализации, авариях в системах энерго-, водо- и теплоснабжения помещение, иных аналогичных случаях, вскрытие служебного помещения осуществляется сотрудником службы безопасности, в соответствии с действующим режимом охраны помещений.

12. По прибытии работников в рабочее (служебное) помещение после нейтрализации нештатных ситуаций, необходимо выполнить мероприятия, указанные в пункте 10 Порядка.

13. Ответственные лица, имеющие доступ в помещения, где размещены используемые СКЗИ, хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ, несут ответственность за неисполнение или ненадлежащее исполнение требований Порядка в соответствии с законодательством Российской Федерации.

ПРИЛОЖЕНИЕ № 4

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области
от 29.05.2020 № [illegible]

ПОРЯДОК
доступа в помещения Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации, в которых ведётся обработка персональных данных

1. Порядок доступа в помещения Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации, в которых ведётся обработка персональных данных (далее — Порядок), определяет требования к доступу в служебные помещения Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее — Министерство) и подведомственной ему организации (далее — подведомственная организация) в целях предотвращения нарушения прав субъектов персональных данных, обрабатываемых в Министерстве и подведомственной организации.

2. Порядок разработан с учётом требований Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами Российской Федерации, регулирующими отношения в области обработки персональных данных.

3. Исполнение настоящего Порядка обязательно для всех лиц, имеющих доступ к персональным данным либо осуществляющих обработку персональных данных в Министерстве и подведомственной организации.

4. Доступ в помещения, в которых ведётся обработка персональных данных, осуществляется с учётом обеспечения безопасности информации в Министерстве и подведомственной организации, а также исключения доступа к персональным данным третьим лицам.

5. Доступ в помещения, в которых ведётся обработка персональных данных, предоставляется:

государственному гражданскому служащему, уполномоченному на обработку персональных данных в Министерстве,

работникам, осуществляющим обработку персональных данных

в Министерстве и подведомственной организации;

администратору информационной безопасности информационных систем Министерства;

иным лицам в случае необходимости по согласованию с Заместителем Председателя Правительства Ульяновской области — Министром агропромышленного комплекса и развития сельских территорий Ульяновской области и руководителем подведомственной организации.

6. В нерабочее время помещения Министерства и подведомственной организации, в которых ведётся обработка персональных данных, хранятся документы и носители информации, содержащие персональные данные, должны закрываться на ключ.

7. Уборка помещений, в которых ведётся обработка персональных данных, хранятся документы и носители информации, содержащие персональные данные, должна производиться в присутствии ответственных лиц Министерства и подведомственной организации, осуществляющих обработку персональных данных.

8. Установка нового оборудования, его замена или ремонт в помещениях, в которых ведётся обработка персональных данных, хранятся документы и носители информации, содержащие персональные данные, должны проводиться по согласованию с ответственным работником за обработку персональных данных и администратором информационной безопасности информационных систем Министерства.

ПРИЛОЖЕНИЕ № 5

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области
от 29.05.2020 № 371

ПОРЯДОК
технического обслуживания, ремонта, модернизации технических и программных средств, входящих в состав информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области

1. Общие положения

1.1. Порядок технического обслуживания, ремонта, модернизации технических и программных средств, входящих в состав информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Порядок) регламентирует взаимодействие структурных подразделений Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и его подведомственной организации (далее – подведомственная организация) по вопросам обеспечения безопасности информации при проведении модификаций программного обеспечения, технического обслуживания средств вычислительной техники, используемой в рамках функционирования информационных систем (далее - ИС) и информационных ресурсов (далее - ИР) Министерства.

1.2. Порядок разработан в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных», Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» и другими нормативными правовыми актами Российской Федерации, регламентирующими отношения в области информационной безопасности.

1.3. Правила, устанавливаемые положениями Порядка обязательны для исполнения всеми пользователями ИС Министерства.

1.4. Все изменения, вносимые в конфигурации технических и программных средств ИС и ИР Министерства, должны производиться только на основании заявок руководителей структурных подразделений Министерства или подведомственной организации, согласованных с администратором

информационной безопасности. информационных систем Министерства (далее – Администратор ИБ ИС Министерства). Перечень изменений, на которые требуется оформление заявки, приведен в пункте 2.2.3 Порядка.

2. Порядок внесения изменений в конфигурации технических и программных средств ИС и ИР Министерства

2.1. Право внесения изменений в конфигурацию аппаратно-программных средств (материнская плата, жесткий диск, дисковод, CD-ROM, DVD-ROM, СЗИ (аппаратные, аппаратно-программные, программные), ПО) рабочих станций и серверов ИС и ИР Министерства предоставляется:

в отношении системных и прикладных программных средств – Администратором ИБ ИС Министерства;

в отношении аппаратных средств - Администратором ИБ ИС Министерства;

в отношении программно-аппаратных средств защиты - Администратором ИБ ИС Министерства;

в отношении программно-аппаратных средств телекоммуникации - Администратором ИБ ИС Министерства;

Изменение конфигурации аппаратно-программных средств рабочих станций и серверов ИС и ИР Министерства кем-либо, кроме Администратора ИБ ИС Министерства, запрещено.

2.2.1. Процедура внесения изменений в конфигурацию аппаратных и программных средств рабочих станций и серверов ИС и ИР Министерства инициируется заявкой руководителя структурного подразделения Министерства или подведомственной организации, либо Администратором ИБ ИС Министерства согласно приложению № 1.

2.2.2. Заявка руководителя структурного подразделения Министерства или подведомственной организации, в которой требуется произвести изменения конфигурации автоматизированного рабочего места (далее – АРМ), оформляется Администратором ИБ ИС Министерства.

Руководитель структурного подразделения, использующего ИС и ИР Министерства, требующих модификации, информируется перед проведением работ.

2.2.3. В заявках могут быть указаны следующие изменения в составе аппаратных и программных средств АРМ и серверов подразделения:

установка в подразделении новой персональная электронная вычислительная машина (далее – ПЭВМ) (развертывание нового АРМ или сервера);

замена ПЭВМ (АРМ или сервера подразделения);

изъятие ПЭВМ (АРМ или сервера подразделения);

добавление устройства (узла, блока) в состав конкретного АРМ или сервера подразделения;

замена устройства (узла, блока) в составе конкретного АРМ или сервера подразделения;

изъятие устройства (узла, блока) из состава конкретного АРМ или сервера;

обновление (восстановление) системного программного обеспечения (далее – ПО);

установка (развертывание) на конкретное АРМ или сервера программных средств, необходимых для решения определенной задачи (добавление возможности решения данной задачи на данном АРМ или сервере), за исключением офисного ПО.

В заявке указываются условные наименования развернутых АРМ и серверов в соответствии с их формулярами (регистрационными карточками). В случае развертывания нового АРМ его наименование в заявке указывать не требуется (оно устанавливается позднее при заполнении формуляра нового АРМ). Наименования задач указываются в соответствии с формулярами задач или перечнем задач архива эталонных дистрибутивов, которые можно решать с использованием ИС и ИР Министерства.

2.2.4. Заключение о технической возможности осуществления затребованных изменений и непосредственного исполнения работ по внесению изменений в конфигурацию АРМ или серверов ИС Министерства проводится Администратором ИБ ИС Министерства.

2.3. Порядок производства работ.

2.3.1. Установка, изменение (обновление) и удаление системных и прикладных программных средств производится Администратором ИБ ИС Министерства. Если АРМ или сервер относится к защищаемым рабочим станциям, то установка и внесение необходимых изменений в настройки средств защиты от несанкционированного доступа и средств контроля целостности файлов (при их использовании) на АРМ осуществляется Администратором ИБ ИС Министерства. В случае необходимости работы производятся в присутствии пользователя данной АРМ.

2.3.3. Подготовка модификаций ПО защищённых серверов и АРМ, тестирование, стендовые испытания и другие необходимые действия производятся Администратором ИБ ИС Министерства.

Установка или обновление подсистем ИС Министерства должны проводиться в строгом соответствии с технологией проведения модификаций программных комплексов данных подсистем.

2.3.4. Модификация ПО серверов осуществляется Администратором ИБ ИС Министерства. При использовании средств защиты информации (далее – СЗИ), после установки модифицированных модулей на сервер Администратор ИБ ИС Министерства устанавливает защиту целостности модулей на сервере (производит пересчёт контрольных сумм эталонов модулей на файл-сервере с помощью средств СЗИ).

2.3.5. Установка и обновление общего ПО (системного, тестового и т.п.)

на рабочие станции и сервера производится с оригинальных лицензионных дистрибутивных носителей (дискет, компакт дисков и т.п.), а прикладного ПО - с эталонных копий программных средств (при реализации сетевого архива эталонных дистрибутивов программ – из него). При необходимости (в случае установки части компонент на дисках сетевых серверов) к работам привлекается Администратор ИБ ИС Министерства.

Все добавляемые программные и аппаратные компоненты должны быть предварительно проверены на работоспособность.

2.3.6. После установки (обновления) ПО Администратор ИБ ИС Министерства должен произвести настройку СЗИ от несанкционированного доступа в соответствии с её (его) формуляром. Настройка должна осуществляться совместно с ответственным пользователем АРМ. Администратор ИБ ИС Министерства должен проверить работоспособность ПО и правильность настройки средств защиты.

После завершения работ по внесению изменений в состав аппаратных средств защищаемого АРМ и его системный блок должен быть опечатан (опломбирован, защищён специальной наклейкой) Администратором ИБ ИС Министерства.

2.3.7. Изъятие АРМ из состава рабочих станций подразделения при её передаче на склад, в ремонт или в другое подразделение осуществляется только после того, как Администратор ИБ ИС Министерства снимет с данной ПЭВМ средства защиты и предпримет необходимые меры для удаления защищаемой информации, которая хранилась на дисках компьютера. Факт уничтожения данных, находившихся на диске компьютера, оформляется актом за подписью Администратора ИБ ИС Министерства согласно приложению № 2. В случае поломки жёсткого диска в договоре, при передаче его в организацию для осуществления ремонта, должна быть предусмотрена ответственность сторонней организации о неразглашении информации, содержащейся на передаваемом диске.

2.3.8 Допуск новых пользователей к решению задач с использованием вновь установленного ПО (либо изменение их полномочий доступа) осуществляется согласно установленным правилам предоставления доступа к ИР Министерства.

2.3.9. Оригиналы документов, на основании которых производились изменения в составе технических или программных средств АРМ с отметками о внесении изменений в состав аппаратно-программных средств, должны храниться у Администратора ИБ ИС Министерства. Они могут использоваться в следующих случаях:

для восстановления конфигурации АРМ после аварий;

для контроля правомерности установки на конкретной АРМ средств для решения соответствующих задач при разборе конфликтных ситуаций;

для проверки правильности установки и настройки средств защиты АРМ.

2.3.10. Регулярные и внеплановые проверки на исправность

и техническое обслуживание технических средств и средств защиты отражать в журнале проверки исправности и технического обслуживания по форме согласно приложению № 3.

3. Экстренная модификация ИС и ИР Министерства

3.1. В исключительных случаях (сбой ПО, не позволяющий продолжить работу), требующих безотлагательного изменения ПО, допускается корректировка программ непосредственно на рабочей станции. В данной ситуации Администратор ИБ ИС Министерства ставит в известность своего начальника отдела информационных технологий и защиты информации ОГБУ «Агентство по развитию сельских территорий Ульяновской области» о необходимости такого изменения.

3.2. Факт внесения изменений в ПО АРМ оформляется актом, который подписывается Администратором ИБ ИС Министерства. В акте указывается причина модификации, перечисляются файлы, подвергшиеся изменению, и указывается лицо(а), осуществившее изменения. При необходимости проводится изменение ПО загрузочного раздела сервера. Если это необходимо, Администратор ИБ ИС Министерства вносит необходимые корректировки в настройки системы контроля целостности ПО АРМ и сервера (при их использовании). Факт модификации ПО и корректировок настроек системы защиты фиксируется на АРМ (сервере).

3.3. В течение следующего дня после составления акта Администратор ИБ ИС Министерства выясняет причины и состав проведенных экстренных изменений и принимают решение о необходимости подготовки исправительной модификации ПО или восстановления ПО АРМ (сервера) с эталонной копии (из АЭД).

Результат расследования оформляется в виде согласованного решения и хранится у Администратора ИБ ИС Министерства.

4. Порядок технического обслуживания и ремонта технических средств АРМ (серверов) ИС.

4.1. Самостоятельное техническое обслуживание и ремонтные работы на технических средствах ПЭВМ АРМ должны осуществляться только Администратором ИБ ИС Министерства. Их вызов осуществляется сотрудниками подразделения, эксплуатирующих АРМ, при возникновении нештатных ситуаций.

4.2. К нештатным ситуациям относятся:

выход из строя или неустойчивое функционирование узлов ПЭВМ или периферийных устройств (например, дисковода, принтера) АРМ;

выход из строя системы электроснабжения АРМ.

4.3. Техническое обслуживание и регламентные работы могут

проводиться в плановом порядке.

4.4. Ответственность за соблюдение требований по обеспечению безопасности информации при проведении технического обслуживания и ремонтных работ на ПЭВМ возлагается на Администратора ИБ ИС Министерства.

4.5. При необходимости осуществления изменений аппаратно-программной конфигурации АРМ соответствующие работы выполняются с соблюдением требований данного Порядка.

5. Порядок проверки работоспособности системы защиты после установки (обновления) программных средств и внесения изменений в списки пользователей

После установки (обновления) программных средств АРМ или внесения изменений в списки пользователей системы Администратор ИБ ИС Министерства обязан проверить работоспособность АРМ и правильность настройки средств защиты, установленных на компьютере в соответствии с инструкциями на конкретные СЗИ.

После осуществления данных действий необходимо проверить корректность функционирования системы защиты.

ПРИЛОЖЕНИЕ № 1
к Порядку технического обслуживания, ремонта, модернизации технических и программных средств, входящих в состав информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области

«___» _____ 20___

ЗАЯВКА
на внесение изменений в состав аппаратно-программных средств ИС и ИР Министерства

Прошу произвести следующие изменения конфигурации аппаратно-программных средств ПЭВМ_____
_____
_____
Наименование структурного подразделения Министерства или подведомственной организации

(развернуть новую рабочую станцию и установить на (обновить на/снять с) неё _____ компоненты), необходимые для решения следующих задач:
_____
_____
_____
_____
_____
_____
_____

Руководитель _____
Наименование структурного подразделения

«___» _____ 20__ _____ _____
Подпись ФИО

Согласовано

«___» _____ 20__ _____ _____
Подпись ФИО

Обратная сторона заявки

Отметка о выполнении
(о внесении изменений в состав аппаратно-программных средств ИС ИР Министерства)

В соответствии с Порядком технического обслуживания, ремонта, модернизации технических и программных средств, входящих в состав информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области _____
Наименование системы

рабочей группой в составе:
администратор информационной безопасности информационных систем Министерства: _____,
от подразделения (отдела) _____
_____

указанные в заявке изменения внесены (не внесены по следующей причине).

_____
Краткое пояснение причины

_____
_____
_____

_____
Изменения в формуляр АРМ (ссылка на данную заявку) внесены.

От администратора информационной безопасности информационных систем Министерства: _____
_____
_____
_____/_____
Подпись, ФИО
«___» _____ 20___

От подразделения _____
_____
_____/_____
Подпись, ФИО

«___» _____ 20___

_____

ПРИЛОЖЕНИЕ № 2
к Порядку технического обслуживания, ремонта, модернизации технических и программных средств, входящих в состав информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области

АКТ
об удалении информации (остаточной), хранившейся на диске компьютера

Все файлы, содержащие подлежащую защите информацию, находившиеся на _____
№_____, передаваемого _____
с какой целью

_____
Кому: должность, ФИО

системного блока ПЭВМ марки _____ серийный №_____ уничтожены (затерты) посредством программы
_____
_____

Администратор информационной безопасности информационных систем Министерства:
_____
_____
_____
_____/_____
Подпись, ФИО
«___» _____ 202__

ПРИЛОЖЕНИЕ № 3
к Порядку технического обслуживания,
ремонта, модернизации технических
и программных средств, входящих в состав
информационных систем и информационных
ресурсов Министерства агропромышленного
комплекса и развития сельских территорий
Ульяновской области

ЖУРНАЛ
проверки исправности и технического обслуживания

№ п/п	Наименование мероприятия	Учетный номер АРМ системного блока	Производимая модернизация, чистка, замена запасных частей (нужное указать)	Дата начала ТО	Дата окончания ТО	Статус (исправен/ не исправен)	Ответственный исполнитель (организатор)
1	1	2	3	4	5	6	7

Ответственный _____

_____

ПРИЛОЖЕНИЕ № 6

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 371

ПОРЯДОК
выявления инцидентов информационной безопасности в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

1.Общие положения

1.1. Порядок выявления инцидентов информационной безопасности в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (далее - Порядок) определяет порядок действий по выявлению и расследованию инцидента информационной безопасности (далее – Инцидент ИБ), устранению его последствий и причин, а также проведения необходимых корректирующих и превентивных мероприятий для ответственных лиц в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и подведомственной ему организации (далее – подведомственная организация).

1.2. Порядок разработан в соответствии с Федеральным законом от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» и иными нормативными правовыми актами, регулирующими общественные отношения в области защиты информации.

1.3. Для целей настоящего Порядка используется следующее понятие:

Инцидент ИБ - событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий информационной безопасности, имеющих значительную вероятность компрометации данных и создания угрозы информационной безопасности.

1.4. Расследование Инцидентов ИБ в Министерстве и подведомственной организации проводится администратором информационной безопасности информационных систем Министерства (далее – Администратор ИБ ИС Министерства) с привлечением в случаях необходимости руководителей и работников структурных подразделений Министерства и подведомственной организации.

Расследование Инцидентов ИБ, затрагивающих два или более подразделения Министерства или подведомственной организации проводится

Администратором ИБ ИС Министерства с привлечением руководителей соответствующих подразделений.

В случае разбирательства по вопросам Инцидентов ИБ, которые затрагивают информационные ресурсы Министерства, Администратор ИБ ИС Министерства в обязательном порядке уведомляет заместителя Председателя Правительства Ульяновской области – Министра агропромышленного комплекса и развития сельских территорий Ульяновской области (далее — Министр).

2. Выявление Инцидента ИБ

2.1. Основными источниками информации об Инцидентах ИБ являются:

факты, выявленные руководителем структурного подразделения Министерства или подведомственной организации, Администратором ИБ ИС Министерства, а также иные работники Министерства и подведомственной организации;

результаты работы средств мониторинга ИБ, а также результаты проверок и аудита (внутреннего или внешнего);

обращения субъектов персональных данных с указанием Инцидента ИБ;

запросы и предписания органов уполномоченных органов за соблюдением прав субъектов персональных данных;

иные источники информации.

2.2. Работник Министерства или подведомственной организации может выявить признаки наличия Инцидента ИБ путём анализа текущей ситуации на предмет её соответствия требованиям, утверждённым в Министерстве и подведомственной организации. Выявленные несоответствия дают основания предполагать факт возникновения Инцидента ИБ. Любые сведения об Инциденте ИБ должны быть незамедлительно переданы выявившим их работником Министерства или подведомственной организации Администратору ИБ ИС Министерства любым доступным способом, в т.ч. через непосредственного руководителя.

3. Анализ исходной информации и принятие решения о проведении расследования Инцидента ИБ

3.1. Администратор ИБ ИС Министерства после получения информации о предполагаемом Инциденте ИБ незамедлительно проводит первоначальный анализ полученных данных. В процессе анализа Администратор ИБ ИС проводит проверку наличия в выявленном факте нарушений.

3.2. По усмотрению руководителя администратора информационной безопасности информационных систем Министерства единичный Инцидент ИБ, не приведший к негативным последствиям и совершенный работником Министерства или подведомственной организации впервые, фиксируется

Администратором ИБ ИС Министерства в карточке данных «Инциденты ИБ» (Приложение) с присвоением статуса «Расследование не требуется».

3.3. В случае наличия признаков Инцидента ИБ в полученной информации Администратор ИБ ИС Министерства определяет предварительную степень важности Инцидента ИБ и принимает решение о необходимости проведения расследования, информирует руководителя администратора информационной безопасности информационных систем Министерства об Инциденте ИБ, инициирует формирование регистрационной карточки инцидента с присвоением ему статуса «В процессе расследования».

3.4. В срок не более 3 (трех) рабочих дней с момента поступления информации об Инциденте ИБ, работник подразделения информационной безопасности по согласованию с руководителем администратора информационной безопасности информационных систем Министерства определяет и инициирует первоочередные меры, направленные на локализацию Инцидента ИБ и на минимизацию его последствий.

3.5. Администратор ИБ ИС Министерства определяет работника, осуществляющего расследование Инцидента ИБ, и передаёт ему всю имеющуюся исходную информацию для проведения расследования, а также информацию о проведенных мероприятиях по локализации Инцидента ИБ.

4. Расследование Инцидента ИБ

4.1. Цели и этапы расследования Инцидента ИБ в Министерстве и подведомственной организации:

4.1.1. Целями разбирательства Инцидентов ИБ являются:

выработка организационных и технических решений, направленных на снижение рисков нарушения информационной безопасности, предотвращение и минимизацию подобных нарушений в будущем;

защита прав Министерства и подведомственной организации в области защиты информации;

защита репутации Министерства и подведомственной организации и его ресурсов;

обеспечение безопасности персональных данных, обрабатываемых в Министерстве и подведомственной организации;

обеспечение прав субъектов персональных данных на обеспечение безопасности и конфиденциальности их персональных данных, обрабатываемых Министерством и подведомственной организацией;

предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации.

4.1.2. Расследование Инцидента ИБ, состоит из следующих этапов:

подтверждение/опровержение факта возникновения Инцидента ИБ;

подтверждение/корректировка уровня значимости Инцидента ИБ;

уточнение дополнительных обстоятельств (деталей) Инцидента ИБ;

получение (сбор) доказательств возникновения Инцидента ИБ, обеспечение их сохранности и целостности;

минимизация последствий Инцидента ИБ;

информирование и консультирование работников Министерства и подведомственной организации по действиям обнаружения, устранения последствий и предотвращения Инцидентов ИБ;

разработка мер по обнаружению и/или предупреждению Инцидентов ИБ.

4.2. При необходимости Администратор ИБ ИС Министерства незамедлительно уведомляет Министра о факте Инцидента ИБ и необходимости создания рабочей группы для проведения расследования Инцидента ИБ.

Администратор ИБ ИС Министерства инициирует подготовку внутреннего документа Министерства о создании рабочей группы в целях расследования указанного Инцидента ИБ, в том числе с указанием сроков расследования Инцидента ИБ, а также при необходимости с определением дополнительных полномочий членов рабочей группы.

4.3. Порядок проведения расследования Инцидента ИБ:

4.3.1. В процессе проведения расследования Инцидента ИБ обязательными для установления являются:

дата и время совершения Инцидента ИБ;

фамилия, имя, отчество, должность и подразделение нарушителя информационной безопасности (далее – Нарушитель ИБ);

уровень критичности Инцидента ИБ;

обстоятельства и мотивы совершения Инцидента ИБ;

информационные ресурсы, затронутые Инцидентом ИБ;

характер и размер реального и потенциального ущерба;

обстоятельства, способствовавшие совершению Инцидента ИБ.

4.3.2. При Инциденте ИБ, затрагивающем не более одного структурного подразделения Министерства или подведомственной организации, Администратор ИБ ИС Министерства информирует о факте Инцидента ИБ руководителя соответствующего подразделения.

4.3.3. При Инциденте ИБ, затрагивающим более одного структурного подразделения Министерства или подведомственной организации, осуществляющий расследование работник информирует руководителей соответствующих подразделений и инициирует проведение расследования с привлечением ресурсов работников отдела информационных технологий и защиты информации ОГБУ «Агентство по развитию сельских территорий Ульяновской области».

4.3.4. В случае проведения временного отключения прав доступа у предполагаемого Нарушителя ИБ информация об отключении прав доступа ответственным за проведение разбирательства направляется руководителю предполагаемого Нарушителя ИБ.

4.3.5. Администратор ИБ ИС Министерства в процессе проведения расследования Инцидента ИБ при необходимости запрашивает информацию в структурных подразделениях, запрос направляется на имя руководителя подразделения Министерства или подведомственной организации с обязательным указанием сроков предоставления информации (с учётом необходимости её анализа, сбора и подготовки).

4.3.6. После получения необходимой информации по Инциденту ИБ осуществляющий расследование Администратор ИБ ИС Министерства проводит анализ полученных данных.

4.3.7. В течение 5 (пяти) рабочих дней с момента назначения осуществляющего расследование Администратора ИБ ИС Министерства (формирования рабочей группы по расследованию Инцидента ИБ), осуществляющий разбирательство Администратор ИБ ИС Министерства запрашивает у руководителя структурного подразделения Министерства или подведомственной организации объяснительную записку Нарушителя ИБ. Объяснительная записка должна быть составлена, подписана Нарушителем ИБ в течение (двух) рабочих дней и представлена его непосредственным руководителем осуществляющему разбирательство Администратору ИБ ИС Министерства в течение 3 (трех) рабочих дней с момента поступления запроса.

В случае отказа Нарушителя ИБ предоставить объяснительную записку, осуществляющему разбирательство Администратору ИБ ИС Министерства предоставляется акт, составленный в соответствии с установленным в Министерстве порядке.

4.3.8. Осуществляющий разбирательство Администратор ИБ ИС проводит оценку негативных последствий от реализации Инцидента ИБ. В ходе данной оценки учитываются:

прямой финансовый ущерб;

репутационный ущерб;

потенциальный ущерб;

косвенные потери, связанные с недоступностью сервисов, потерей информации;

другие виды ущерба или аспекты негативных последствий для Министерства, подведомственной организации или субъектов персональных данных.

4.3.9. С целью минимизации последствий Инцидента ИБ возможно временное отключение прав доступа работника Министерства или подведомственной организации к информационным ресурсам Министерства на время проведения расследования, предварительно оформив заявку. Подобное отключение инициируется осуществляющим расследование Администратором ИБ ИС Министерства с обязательным предварительным устным согласованием с непосредственным руководителем сотрудника Министерства или подведомственной организации.

4.3.10. В случае, если у Нарушителя ИБ были отключены права доступа к информационным ресурсам на время проведения расследования, то по его результатам осуществляющий расследование Администратор ИБ ИС Министерства по согласованию с непосредственным руководителем Нарушителя ИБ принимает решение и инициирует возвращение в полном или ограниченном объёме ранее имеющихся у Нарушителя ИБ прав доступа к мнформационным ресурсам либо инициирует официальную процедуру отмены (изменения) прав доступа к информационным ресурсам. Если Инцидент ИБ было вызвано незнанием Нарушителем ИБ правил (технологии) работы с информационными ресурсами Министерства, то основанием для возврата прав доступа является успешное прохождение Нарушителем ИБ повторного инструктажа, проведенного Администратором ИБ ИС Министерства, ознакомлением с положениями инструкций в сфере защиты информации и иными внутренними документами Министерства в области защиты информации.

4.3.11. Восстановление временно отключенных у Нарушителя ИБ прав доступа к информационным ресурсам (разблокировка пользователя) может производиться только по заявке непосредственного руководителя Нарушителя ИБ или осуществляющего расследование работника.

5. Оформление результатов проведённого расследования

5.1. Собранная в процессе расследования Инцидента ИБ информация фиксируется осуществляющим расследование Администратором ИБ ИС Министерства в картотеке данных «Инциденты ИБ» и учитывается при подготовке итогового заключения по Инциденту ИБ.

5.2. Осуществляющий расследование работник формирует, согласовывает со всеми участниками расследования и подписывает итоговое заключение по расследованию Инцидента ИБ.

5.3. Итоговое заключение по Инциденту ИБ осуществляющий разбирательство Администратор ИБ направляет заинтересованным руководителям структурных подразделений Министерства или подведомственной организации.

5.4. Осуществляющий расследование Администратор ИБ ИС Министерства фиксирует завершение расследования в карточке «Инциденты ИБ» и присваивает Инциденту ИБ статус «Разбирательство завершено».

5.5. Осуществляющий разбирательство Администратор ИБ ИС Министерства, при необходимости определения правовой оценки Инцидента ИБ, может обратиться за консультациями в отдел правовой и организационной работы Министерства. В этом случае информацию по Инциденту ИБ осуществляющий расследование Администратор ИБ ИС Министерства передаёт с грифом «Конфиденциально» от руководителя

администратора информационной безопасности информационных систем Министерства

О результатах проведенного анализа и других мероприятий, отдел правовой и организационной работы Министерства в течение не более 5 (пяти) рабочих дней после получения запроса информирует руководителя администратора информационной безопасности информационных систем Министерства.

5.6. В случае выявления в Инциденте ИБ признаков административного правонарушения или уголовного преступления, относящихся к сфере информационных технологий, осуществляющий расследование Администратор ИБ передаёт все материалы по Инциденту ИБ руководству Министерства в целях подачи соответствующего заявления в правоохранительные органы Российской Федерации, уполномоченные рассматривать данную сферу правоотношений.

5.7. Осуществляющий расследование Администратор ИБ ИС Министерства фиксирует полученную дополнительную информацию в карточке данных «Инциденты ИБ» и информирует ведущего консультанта по мобилизационной работе Министерства.

6. Завершение расследования Инцидента ИБ, превентивные мероприятия

6.1. По завершению расследования Инцидента ИБ, осуществляющий разбирательство Администратор ИБ ИС Министерства передаёт имеющиеся материалы (в объёме, достаточном для принятия решения) вышестоящему руководителю Нарушителя ИБ для решения вопроса о целесообразности привлечения Нарушителя ИБ к дисциплинарной ответственности.

6.2. На основании полученных результатов расследования руководитель структурного подразделения в срок не более 3 (трех) рабочих дней организовывает проведение одного или нескольких мероприятий, направленных на снижение рисков информационной безопасности в будущем:

повторное ознакомление Нарушителя ИБ с требованиями внутренних документов Министерства в сфере защиты информации;

анализ и пересмотр имеющихся прав доступа к информационным ресурсам у Нарушителя ИБ;

доведение до всех работников структурного подразделения требований внутренних нормативных документов Министерства:

обсуждение Инцидента ИБ на совещании руководителей или собрании коллектива Министерства и подведомственной организации;

отмена неактуальных прав доступа к информационным ресурсам;

проведение мероприятий, направленных на предотвращение несанкционированного доступа к персональным данным и (или) передачи их лицам, не имеющим права доступа к такой информации;

иные обоснованные меры.

6.3. О результатах проведённого расследования Инцидента ИБ Администратор ИБ ИС Министерства по необходимости инициирует подготовку сообщения об Инциденте ИБ в адрес Министра.

7. Права, обязанности и ответственность участников расследования Инцидента ИБ

7.1. Осуществляющий расследование Администратор ИБ ИС Министерства имеет право:

7.1.1. По согласованию с непосредственным руководителем Нарушителя ИБ требовать предоставлений письменных объяснений по обстоятельствам Инцидента ИБ у Нарушителя ИБ.

7.1.2. Запрашивать и получать от руководителей и работников Министерства и подведомственной организации, в рамках их компетенций, устные и письменные разъяснения и иную информацию, необходимую для проведения расследования Инцидента ИБ.

7.1.3. Инициировать на основании заявок отключение от информационных ресурсов работников Министерства или подведомственной организации, нарушивших правила или требования информационной безопасности, на период проведений расследования Инцидента ИБ в случае если имеется существенный риск того, что продолжение работы работника с информационными ресурсами может повлечь значительное увеличение ущерба или новые инциденты информационной безопасности.

7.1.4. По результатам расследования Инцидента ИБ инициировать изменения в бизнес-процессах и информационных ресурсах Министерства с целью повышения их защищённости и снижения рисков Инцидентов ИБ.

7.1.5. Инициировать процедуры привлечения Нарушителя ИБ к дисциплинарной/ материальной ответственностью согласно внутренним документам Министерства.

7.2. Осуществляющий разбирательство Администратор ИБ ИС Министерства обязан:

7.2.1. Объективно и основательно проводить расследование каждого Инцидента ИБ.

7.2.2. Определять первоочередные меры, направленные на локализацию Инцидента ИБ и минимизацию негативных последствий.

7.2.3. Фиксировать в карточке данных «Инциденты ИБ» всю исходную информацию об Инциденте ИБ и результаты его расследования.

7.2.4. Предоставлять отчёты и рекомендации по проведённым расследованиям руководству подразделения информационной безопасности.

7.2.5. Проводить анализ обстоятельств, способствовавших совершению каждого Инцидента ИБ, и на его основе, совместно с сотрудниками смежных подразделений, разрабатывать рекомендации и предложения по оптимизации деятельности Министерства и подведомственной организации в области

защиты информации, снижения ущерба от подобных Инцидентов ИБ и минимизации возможности их повторения в будущем.

7.2.6. Составление заключений по фактам несоблюдения условий хранения носителей персональных данных, использования средств защиты информации, приводящим к снижению уровня защищённости персональных данных, разработку и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

7.3. Руководители и работники Министерства обязаны:

7.3.1. Предоставлять по запросам проводящего расследования Администратора ИБ ИС Министерства устные и письменные разъяснения и иную информацию в рамках своей компетенции, необходимую для проведения расследования Инцидента ИБ;

7.3.2. Информировать Администратора ИБ ИС Министерства о выявленных Инцидентах ИБ;

7.3.3. Информировать Администратора ИБ ИС Министерства об имеющихся запросах и обращениях субъектов персональных данных.

ПРИЛОЖЕНИЕ
к Порядку выявления инцидентов информационной безопасности в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

Карточка данных о инциденте информационной безопасности

Дата события
Номер события

Стр. 1

Информация о сообщающем лице

ФИО _____ Адрес _____

Организация _____ _____

Телефон _____ Электронная почта _____

Описание события информационной безопасности

Описание события:

☐ Что произошло
☐ Как произошло
☐ Почему произошло
☐ Пораженные компоненты
☐ Негативное воздействие на бизнес
☐ Любые идентифицированные уязвимости

Детали события информационной безопасности

Дата и время возникновения события
Дата и время обнаружения события

Дата и время сообщения о событии

Закончилось ли событие? *(отметить квадрат)* Да ☐ **Нет** ☐

Если «да», то уточнить, как долго длилось событие в днях/часах/минутах

Дата инцидента
Номер инцидента

Информация о сотруднике группы обеспечения эксплуатации

Фамилия	_____	Адрес	_____
Телефон	_____	Электронная почта	_____

Информация о сотруднике ISIRT

Фамилия	_____	Адрес	_____
Телефон	_____	Электронная почта	_____

Описание инцидента информационной безопасности

Дальнейшее описание инцидента:

☐ Что произошло
☐ Как произошло
☐ Почему произошло
☐ Пораженные компоненты
☐ Негативное воздействие на бизнес
☐ Любые идентифицированные уязвимости

Детали инцидента информационной безопасности

Дата и время возникновения инцидента

Дата и время обнаружения инцидента

Дата и время сообщения об инциденте

Закончился ли инцидент? *(отметить квадрат)* **Да** ☐ Нет ☐

Если «да», то уточнить, как долго длился инцидент в днях/часах/минутах. Если «нет», то уточнить, как долго он уже длится

Тип инцидента ИБ

(Отметить один квадрат, затем заполнить соответствующие поля ниже) **Действительный** ☐ **Попытка** ☐ **Подозрение** ☐

(Один из) **Намеренная** ☐ *(указать типы угрозы)*

Хищение (TH) ☐
Мошенничество (FR) ☐
Саботаж/физический ущерб (SA) ☐
Вредоносная программа (MC) ☐
Хакерство/Логическое проникновение (HA) ☐
Неправильное использование ресурсов (MI) ☐
Другой ущерб (OD) ☐

Определить:

(Один из) **Случайная** ☐ *(указать типы угрозы)*

Отказ аппаратуры (HF) ☐
Отказ ПО (SF) ☐
Отказ связи (CF) ☐
Пожар (HE) ☐
Наводнение (FL) ☐
Другие природные события (NE) ☐

Определить:

Потеря существенных сервисов (LE) ☐
Недостаточное кадровое обеспечение (SS) ☐
Другие случаи (OA) ☐

Определить:

(Один из) **Ошибка** ☐ *(указать типы угрозы)*

Операционная ошибка (OE) ☐
Ошибка аппаратной поддержки (HE) ☐
Ошибка поддержки ПО (SE) ☐
Ошибка пользователя (UE) ☐
Ошибка конструкции (DE) ☐
Другие случаи (включая истинные заблуждения) (OA) ☐

Определить:

Неизвестно ☐

(Если еще не установлен тип инцидента (намеренный, случайный, ошибка), то следует отметить квадрат «неизвестно» и, по возможности, указать тип угрозы, используя сокращения, приведенные выше)
Определить:

Пораженные активы

Пораженные активы (если есть)

(Дать описания активов, пораженных инцидентом, или связанных с ним, включая серийные, лицензионные номера и номера версий, по возможности)

Информация/Данные _____

Аппаратура _____

Программное обеспечение _____

Средства связи _____

Документация _____

Негативное воздействие/влияние инцидента на бизнес

Отметить соответствующие квадраты для указанных ниже нарушений, затем в колонке «значимость» указать уровень негативного воздействия на бизнес по шкале 1□10, используя сокращения (указатели категорий): (FD) – финансовые потери/разрушение бизнес-операций, (CE) – коммерческие и экономические интересы, (PI) – информация, содержащая персональные данные, (LR) – правовые и нормативные обязательства(это необходимо сличить с английским оригиналом),(MO) – менеджмент и бизнес-операции, (LG) – потеря престижа Запишите кодовые буквы в колонке «указатели», а если известны действительные стоимости, то указать их в колонке «стоимость»

		Значимость	Указатели	Стоимость
Нарушение конфиденциальности *(т. е., несанкционированное раскрытие)*	□			
Нарушение целостности *(т. е., несанкционированная модификация)*	□			
Нарушение доступности *(т. е., недоступность)*	□			
Нарушение неотказуемости	□			
Уничтожение	□			

Полные стоимости восстановления после инцидента

(Где возможно, необходимо указать общие расходы на восстановление после инцидента в целом по шкале 1□10 для «значимости» и в деньгах для «стоимости»)	Значимость	Указатели	Стоимость

Разрешение инцидента

Дата начала расследования инцидента _____

Фамилия лица (лиц), проводившего (их) расследование инцидента _____

Дата окончания инцидента _____

Дата окончания воздействия _____

Дата завершения расследования инцидента _____

Ссылка и место хранения отчета о расследовании _____

Причастные лица

(Один из)

Лицо (PE) ☐

Организованная группа (GR) ☐

Легально учрежденная организация/учреждение (OI) ☐

Случайность (AC) ☐

Нет виновного (NP) ☐
Например, природные факторы, отказ оборудования, ошибка человека

Описание нарушителя

Действительная или предполагаемая мотивация

(Один из)

Криминальная/финансовая выгода(CG) ☐

Политика/Терроризм (PT) ☐

Развлечение/хакерство (PH) ☐

Реванш (RE) ☐

Другие мотивы (OM) ☐

Определить:

Действия, предпринятые для разрешения инцидента

(например, «никаких действий», «подручными средствами», «внутреннее расследование», «внешнее расследование с привлечением...»)

Действия, запланированные для разрешения инцидента

(например, см. выше)

Прочие действия

(например, по-прежнему требуется проведение расследования для другого персонала)

Заключение

(Отметить один из квадратов, является ли инцидент значительным или нет и добавить в краткое объяснение для обоснования этого заключения)

Значительный ☐ **Незначительный** ☐

(Укажите любые другие заключения) _____

Ознакомленные лица/субъекты

(Эта часть отчета заполняется соответствующим лицом, на которое возложены обязанности в области ИБ и которое формулирует требуемые действия. Обычно этим лицом является руководитель ИБ организации).

Руководитель ИБ	☐	Ответственный за ИБ Министерства	☐
Местный руководитель (уточнить, какого подразделения)	☐	Руководитель информационных систем	☐
Автор отчета	☐	Руководитель автора отчета	☐
		Другое лица	☐

(например, справочная служба, отдела кадров, менеджмента, внутреннего аудита, регулятивного органа, сторонняя КСБР)

Определить:

Привлеченные лица

Инициатор		Работник		Работник	
Подпись	_____	Подпись	_____	Подпись	_____
Фамилия	_____	Фамилия	_____	Фамилия	_____
Роль	_____	Роль	_____	Роль	_____
Дата	_____	Дата	_____	Дата	_____

Работник		Работник		Работник	
Подпись	_____	Подпись	_____	Подпись	_____
Фамилия	_____	Фамилия	_____	Фамилия	_____
Роль	_____	Роль	_____	Роль	_____
Дата	_____	Дата	_____	Дата	_____

ПРИЛОЖЕНИЕ № 7

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 371

ИНСТРУКЦИЯ
по восстановлению связи в случае компрометации действующих ключей к средствам криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

1. Инструкция по восстановлению связи в случае компрометации действующих ключей к средствам криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (далее - Инструкция) определяет порядок действий по восстановлению связи в случае компрометации действующих ключей к средствам криптографической защиты информации (далее - СКЗИ) в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и подведомственной ему организации (далее – подведомственная организация).

2. Для целей настоящей Инструкции используется следующее понятие:

Компрометация индивидуального ключа - утрата доверия к тому, что используемые ключи обеспечивают безопасность конфиденциальной информации.

3. К событиям, связанным с компрометацией действующих криптографических ключей, относится:

3.1. Утрата (в том числе хищение) ключевых дискет (флэш - накопителей) с последующим их обнаружением;

3.2. Увольнение пользователей, имевших доступ к ключевой информации;

3.3. Передача ключевой информации по линии связи в открытом виде в случае, если это не предусмотрено правилами пользования;

3.4. Нарушение правил хранения и уничтожения (после окончания срока действия) секретного ключа;

3.5. Возникновение подозрений на утечку информации или её искажение;

3.6. Не расшифровывание входящих или исходящих сообщений;

3.7. Отрицательный результат при проверке электронной цифровой подписи документа;

3.8. Нарушение целостности упаковки ключевых дискет (флэш - накопителей) и (или) печати на сейфе, где хранились ключевые дискеты (флэш - накопители);

3.9. Несанкционированное копирование ключевых дискет (флэш - накопителей);

3.10. Случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе, случаи, когда магнитный носитель вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате злоумышленных действий).

4. События, указанные в подпунктах 3.1 – 3.5 пункта 3 Инструкции, должны трактоваться, как безусловная компрометация действующих ключей. При наличии событий, указанных в подпунктах 3.6 – 3.10 пункта 3 Инструкции, требуется специальное расследование в каждом конкретном случае.

5. При наступлении любого из перечисленных событий, указанных в подпунктах 3.1 – 3.10 пункта 3 Инструкции, ответственный работник Министерства или подведомственной организации (далее – Пользователь СКЗИ) должен немедленно прекратить связь с другими работниками Министерства или подведомственной организации и сообщить о факте компрометации (или предполагаемом факте компрометации) ответственному за эксплуатацию СКЗИ.

6. Расследование факта компрометации (или предполагаемой компрометации) должно проводиться на месте происшествия специально назначаемой комиссией под председательством ответственного за эксплуатацию СКЗИ.

Результатом рассмотрения является квалификация или не квалификация данного события, как компрометация действующих ключей к СКЗИ.

При установлении факта компрометации действующих ключей скомпрометированные секретные ключи шифрования и электронной подписи уничтожаются.

7. Для восстановления конфиденциальной связи после компрометации ключей Пользователь СКЗИ обращается к ответственному за эксплуатацию СКЗИ с целью регистрации вновь изготовленных (или резервных) ключей. Регистрация новых ключей шифрования и электронной подписи осуществляется тем же порядком, как и при плановой смене ключей.

8. Пользователь СКЗИ несёт персональную ответственность:

8.1. За правильность эксплуатации и сохранность СКЗИ носителей ключевой информации и других документов о ключах, выдаваемых с ключевыми носителями;

8.2. За сохранение в тайне конфиденциальной информации, ставшей им известной в процессе работы с СКЗИ;

8.3. За сохранение в тайне содержания закрытых ключей СКЗИ и средств электронной подписи;

8.4. За утрату и некорректность эксплуатации СКЗИ и закрытых ключей;

8.5. За то, чтобы на компьютере, на котором установлены СКЗИ и средства электронной подписи, не были установлены и не эксплуатировались программы (в том числе вирусы), которые могут нарушить функционирование программных СКЗИ и средств электронной подписи;

8.6. В случае несвоевременного сообщения о факте компрометации ключей.

Пользователь СКЗИ, допустивший компрометацию ключей, несёт ответственность в полном объёме за ущерб, причиненный им другим работникам системы.

Пользователь СКЗИ, допустивший компрометацию ключей, несёт ответственность за неисполнение или ненадлежащее исполнение своих обязанностей в соответствии с законодательством Российской Федерации.

ПРИЛОЖЕНИЕ № 8

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 377

ИНСТРУКЦИЯ
пользователя информационных систем Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области

1. Общие положения

1.1. Инструкция пользователя информационных систем Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Инструкция) определяет порядок работы работников Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и подведомственной ему организации (далее – подведомственная организация) в защищённой от несанкционированного доступа информационных системах Министерства.

1.2. Для целей настоящей Инструкции ответственный работник Министерства или подведомственной организации (далее - Пользователь) в рамках своих функциональных обязанностей участвует в процессах автоматизированной обработки информации в информационных системах Министерства.

1.3. Пользователь в своей работе руководствуется нормативными правовыми актами Российской Федерации, регулирующими отношения в области функционирования информационных систем, настоящей Инструкцией и другими правовыми документами Министерства.

1.4. Методическое руководство работой Пользователя осуществляется ответственным за организацию работ по защите информации в Министерстве.

2. Обязанности Пользователя

2.1. Пользователь отвечает за правильность действий при работе с информационной системой Министерства, в том числе действий при входе в систему.

2.2. Допуск Пользователей для работы на автоматизированном рабочем месте (далее - АРМ) осуществляется после прохождения инструктажа по работе с информационными системами и информационными ресурсами Министерства.

2.3. В процессе первичной регистрации Пользователя руководитель подразделения Министерства или подведомственной организации, в котором работает Пользователь, заявляет Администратору информационной безопасности информационных сетей Министерства (далее – Администратор ИБ ИС Министерства) перечень необходимых для работы пользователя ресурсов, перечень персональных данных, состав необходимого общесистемного программного обеспечения для решения поставленных задач.

2.4. Обо всех выявленных нарушениях, связанных с информационной безопасностью информационных систем Министерства, а также для получений консультаций по вопросам информационной безопасности, необходимо обратиться к Администратору ИБ ИС Министерства по электронной почте: it@mcx73.ru или по внутреннему телефону +7 (8422) 73-56-79.

2.5. Пользователь обязан:

2.5.1. Знать и выполнять установленные требования действующих нормативных правовых актов Российской Федерации, регулирующих отношения в области функционирования информационных систем, настоящей Инструкции и других правовых документов Министерства.

2.5.2. Выполнять на АРМ только те процедуры, которые определены для него в должностной инструкции.

2.5.3. Знать и соблюдать требования по режиму обработки персональных данных, учёту, хранению и пересылке носителей информации, обеспечению безопасности служебной информации.

2.5.4. Соблюдать правила при работе в сетях общего доступа и (или) международного обмена (информационно-телекоммуникационной сети «Интернет» и других) (далее - Сеть).

2.5.5. При работе со съёмными носителями каждый раз перед началом работы проверить их на наличие вирусов с использованием штатных антивирусных программ. В случае обнаружения вирусов на машинных носителях информации (съёмных носителях, жёстком магнитном диске, твердотельном носителе) пользователь обязан немедленно сообщить Администратору ИБ ИС Министерства.

2.5.6. В случае оставления рабочей станции без визуального контроля доступ к компьютеру должен быть немедленно заблокирован. Для этого Пользователю необходимо нажать одновременно комбинацию клавиш <Ctrl><Alt><Del> и выбрать опцию <Блокировка>, либо комбинацией клавиш Win + L.

2.5.7. Принимать меры по реагированию, в случае возникновения внештатных ситуаций и аварийных ситуаций, с целью ликвидации их последствий, в пределах, возложенных на него функций.

2.6. Пользователю запрещается:

2.6.1. Разглашать защищаемую информацию Министерства и подведомственной организации третьим лицам.

2.6.2. Копировать защищаемую информацию на внешние носители без разрешения руководителя подразделения Министерства или подведомственной организации.

2.6.3. Самостоятельно устанавливать, тиражировать, или модифицировать программное обеспечение и аппаратное обеспечение, изменять установленный алгоритм функционирования технических и программных средств.

2.6.4. Несанкционированно открывать общий доступ к папкам на своей рабочей станции.

2.6.5. Подключать к рабочей станции и корпоративной информационной сети личные внешние носители и мобильные устройства.

2.6.6. Отключать (блокировать) средства защиты информации.

2.6.7. Обрабатывать на АРМ информацию и выполнять другие работы, не предусмотренные перечнем прав пользователя по доступу к информационной системе Министерства.

2.6.8. Сообщать (или передавать) посторонним лицам личные ключи и атрибуты доступа к ресурсам информационной системы Министерства.

2.6.9. Привлекать посторонних лиц для производства ремонта или настройки АРМ, без согласования с ответственным за обеспечение защиты персональных данных в Министерстве.

2.6.10. Самостоятельно вносить изменения в аппаратно-программную конфигурацию информационных систем Министерства, изменять месторасположение средств отображения информации.

2.7. Пользователь несёт ответственность за неисполнение или ненадлежащее исполнение обязанностей, а также за несоблюдение запретов, изложенных в настоящей Инструкции, в соответствии с законодательством Российской Федерации.

3. Правила работы Пользователя в Сети

3.1. Работа в Сетях на элементах информационных систем Министерства должна проводиться при служебной необходимости.

3.2. При работе в Сети запрещается:

3.2.1. Осуществлять работу при отключенных средствах защиты (антивирус и других).

3.2.2. Передавать по Сети защищаемую информацию без использования механизмов защиты.

3.2.3. Скачивать из Сети программное обеспечение и другие файлы.

3.2.4. Посещение сайтов сомнительной репутации.

3.2.5. Нецелевое использование подключения к Сети.

ПРИЛОЖЕНИЕ № 9

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 371

ИНСТРУКЦИЯ
администратора безопасности информационных систем Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области

1. Общие положения

1.1. Инструкция администратора информационной безопасности информационных систем Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее – Инструкция) определяет функции, права и обязанности администратора информационной безопасности информационных систем Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее – Администратор ИБ ИС Министерства) по вопросам обеспечения информационной безопасности при подготовке и исполнении документов в информационной системе (далее - ИС) Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство).

1.2. Администратор ИБ ИС Министерства руководствуется нормативным правовыми актами Российской Федерации, регулирующими отношения в обеспечении защиты информации.

1.3. Администратор ИБ ИС Министерства назначается распоряжением Министерства и обеспечивает правильность использования и нормальное функционирование установленной системы защиты ИС Министерства.

1.4. Администратор ИБ обладает правами доступа к любым программно-аппаратным средствам защиты информации (далее – СЗИ) на технических средствах работников Министерства и подведомственной ему организации (далее – подведомственная организация).

2. Обязанности Администратора ИБ ИС Министерства

2.1. Администратор ИБ ИС Министерства обязан:

2.1.1. Осуществлять учёт и периодический контроль за составом и полномочиями работников ИС Министерства.

2.1.2. Осуществлять оперативный контроль за работой работников ИС Министерства, анализировать содержимое системных журналов средств

вычислительной техники (далее – СВТ) и адекватно реагировать на возникающие нештатные ситуации.

2.1.3. Обеспечивать своевременное архивирование системных журналов СВТ и надлежащий режим хранения данных архивов.

2.1.4. Осуществлять непосредственное управление режимами работы и административную поддержку функционирования применяемых в ИС Министерства СЗИ.

2.1.5. Присутствовать при внесении изменений в конфигурацию (модификации) аппаратно-программных средств защищённых СВТ, обеспечивать и контролировать установку и настройку СЗИ.

2.1.6. Не реже одного раза в месяц проверять состояние используемых СЗИ, осуществлять проверку правильности их настройки (выборочное тестирование).

2.1.7. Управлять учётными записями пользователей, реализовывать правила разграничения доступа, а также осуществлять контроль соблюдения этих правил в соответствии с Инструкцией по организации парольной защиты при работе с информационными системами и устройствами в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации.

2.1.8. Управлять идентификаторами (осуществлять создание, присвоение и уничтожение идентификаторов пользователей и устройств) и средствами аутентификации (аутентификационной информацией) штатных работников в ИС Министерства, обеспечивать соблюдение правил идентификации и аутентификации работников и устройств.

2.1.9. Осуществлять контроль за хранением, выдачей, инициализацией, блокированием средств аутентификации и принятием мер в случае утраты и (или) компрометации средств аутентификации в соответствии с Инструкцией по организации парольной защиты при работе с информационными системами и устройствами в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации.

2.1.10. Осуществлять контроль не реже одного раза в три месяца установленного (инсталлированного) в ИС Министерства программного обеспечения.

2.1.11. Настраивать параметры журналов регистрации событий безопасности.

2.1.12. Проводить мониторинг и анализ результатов регистрации событий безопасности и реагирование на них не реже одного раза в неделю.

2.1.13. Управлять средствами антивирусной защиты в соответствии с Инструкцией по антивирусной защите информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области.

2.1.14. Осуществлять контроль уровня защищённости информации, обрабатываемой в ИС Министерства.

2.1.15. Осуществлять контроль выполнения условий и сроков действия сертификатов соответствия на СЗИ и принятие мер, направленных на устранение выявленных недостатков.

2.1.16. Обеспечивать сохранность СЗИ, эксплуатационной и технической документации к СЗИ, а также порядок обращения с СЗИ в процессе получения, хранения, доставки, передачи, встраивания в прикладные системы, тестирования в целях защиты информации, обрабатываемой с использованием средств автоматизации в соответствии с Порядком эксплуатации средств криптографической защиты информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации.

2.1.17. Проводить не реже одного раза в шесть месяцев контроль правил генерации и смены паролей пользователей, заведения и удаления учётных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в соответствии с Инструкцией по организации парольной защиты при работе с информационными системами и устройствами в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации.

2.1.18. Своевременно и точно отражать изменения в организационно-распорядительных документах по управлению СЗИ, установленных на СВТ ИС Министерства.

2.1.19. Осуществлять поэкземплярный учёт в соответствующем журнале: СЗИ (носителей дистрибутивов, системных блоков с установленными СЗИ), а также эксплуатационной и технической документации к СЗИ.

2.1.20. Осуществлять хранение носителей дистрибутивов СЗИ, а также лицензий и сертификатов на СЗИ.

2.1.21. Не реже одного раза в месяц осуществлять проверки состояния защищённости информационных ресурсов от сбоев в системе электропитания (система резервирования и автоматического ввода резерва), а также проверки состояния линейно-кабельного оборудования локально-вычислительных сетей (наличие запирающих и опечатывающих устройств, оборудования распределительных шкафов).

2.1.22. Проводить первоначальный, плановый и внеплановый инструктаж обслуживающего и эксплуатирующего персонала ИС Министерства по вопросам работы с СЗИ.

2.1.23. Консультировать обслуживающего и эксплуатирующего персонала ИС Министерства по вопросам, связанным с работой СЗИ.

2.1.24. Разрабатывать инструкции по работе с СЗИ.

2.1.25. Докладывать руководству Министерства и подведомственной организации об имевших место попытках несанкционированного доступа к информации и техническим средствам ИС.

2.1.26. Участвовать в выявлении инцидентов информационной безопасности и реагировании на них.

В ходе выявления инцидентов и реагирования на них осуществляются следующие мероприятия:

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

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

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

планирование и принятие мер по предотвращению повторного возникновения инцидентов;

2.1.27. Управлять системой защиты информации ИС Министерства, в ходе которой осуществляются следующие мероприятия:

поддержание системы защиты информации (структуры системы защиты информации ИС Министерства, состава, мест установки и параметров настройки средств защиты информации, программного обеспечения и технических средств) в соответствии с эксплуатационной документацией на систему защиты;

управление изменениями системы защиты информации, в том числе определение типов возможных изменений системы защиты информации, санкционирование внесения изменений в системы защиты информации, документирование действий по внесению изменений в системы защиты информации, сохранение данных об изменениях системы защиты информации, контроль действий по внесению изменений в системы защиты информации;

анализ потенциального воздействия планируемых изменений в системы защиты информации на обеспечение защиты информации, возникновение дополнительных угроз безопасности информации и работоспособность ИС Министерства;

определение параметров настройки программного обеспечения, включая программное обеспечение средств защиты информации, состава и конфигурации технических средств и программного обеспечения до внесения изменений в базовую конфигурацию ИС Министерства и их системы защиты информации;

внесение информации (данных) об изменениях в базовой конфигурации ИС Министерства и их системы защиты информации в эксплуатационную документацию на систему защиты информации ИС Министерства.

2.1.28. В случае возникновения нештатных ситуаций и аварийных ситуаций принимать меры по реагированию в пределах функций и полномочий с целью ликвидации последствий.

2.1.29. Оперативно докладывать руководству Министерства и подведомственной организации о случаях возникновения внештатных ситуаций и аварийных ситуаций.

2.1.30. В кратчайшие сроки принимать меры по восстановлению работоспособности элементов ИС Министерства. Предпринимаемые меры по возможности согласовывать с вышестоящим руководством Министерства и подведомственной организации.

3. Права Администратора ИБ ИС Министерства

3.1. Администратор ИБ ИС Министерства имеет право:

3.1.1. Проводить служебные расследования по фактам нарушения установленных требований обеспечения информационной безопасности, несанкционированного доступа, утраты, порчи защищаемой информации и технических компонентов ИС Министерства.

3.1.2. Непосредственно обращаться к пользователям АРМ с требованием прекращения работы в ИС Министерства при несоблюдении установленной технологии обработки информации и невыполнении требований по безопасности.

3.1.3. В пределах своей компетенции сообщать руководству Министерства и подведомственной организации обо всех недостатках в работе ИС Министерства и их системы защиты.

3.1.4. Требовать от руководства Министерства и подведомственной организации обеспечения организационно-технических условий, необходимых для исполнения обязанностей.

3.1.5. Подписывать и визировать документы в пределах своих обязанностей в соответствии с настоящей Инструкцией.

3.1.6. Получать доступ к информации, материалам, техническим средствам, помещениям, необходимый для надлежащего исполнения своих прав и обязанностей (в том числе вести мониторинг действий пользователей и обслуживающего персонала ИС Министерства).

3.1.7. Вносить свои предложения по совершенствованию мер защиты информации в ИС Министерства.

4. Ответственность Администратора ИБ ИС Министерства

Администратор ИБ ИС Министерства несёт ответственность за неисполнение или ненадлежащее исполнение должностных обязанностей в соответствии с законодательством Российской Федерации.

ПРИЛОЖЕНИЕ № 10

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 371

ИНСТРУКЦИЯ
по организации парольной защиты при работе с информационными системами и устройствами в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

1. Общие положения

1.1. Инструкция по организации парольной защиты при работе с информационными системами и устройствами в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (далее - Инструкция) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учётных записей работников) в рамках работы с информационными системами (далее - ИС) и устройствами, содержащие информационные ресурсы (далее - Устройства), при обработке служебной информации и персональных данных в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и подведомственной ему организации (далее – подведомственная организация), а также контроль за действиями работников Министерства и подведомственной организации, обслуживающего персонала ИС и Устройств при работе с паролями.

1.2. Идентификация/аутентификация работников, как пользователей ИС Министерства, осуществляется посредством использования паролей.

1.3. Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех подсистемах автоматизированной системы Министерства и контроль за действиями работников Министерства и подведомственной организации, обслуживающего персонала ИС при работе с паролями возлагается на Администратора информационной безопасности информационных систем Министерства (далее – Администратор ИБ ИС Министерства).

2. Правила формирования и работы с паролями

2.1. Доступ к информационным активам в Министерстве и подведомственной организации должен производиться с использованием персональных учётных записей и периодически сменяемых буквенно-цифровых паролей, удовлетворяющих следующим требованиям:

пароль содержит не менее восьми символов, включая буквы обоих регистров и цифры;

не является словом, присутствующим в словарях, или профессиональным термином, в том числе набранным в другой раскладке клавиатуры;

не основывается на семейной, служебной и другой легко доступной информации (фамилии, имена, даты рождения, клички животных, автомобильные и телефонные номера, названия организаций, адреса сайтов и др.);

не содержит легко угадываемые последовательности символов (например, 123456, aaabbb, qwerty, q1w2e3);

одним из способов создания безопасных, но легко запоминающихся паролей является кодирование стихотворной строки или осмысленного утверждения. Так, пароль, созданный на основе фразы: «Вот один пример надежного и запоминающегося пароля», может быть таким: «VotlPN&ZP».

2.2. Внеплановая смена личного пароля или удаление учётной записи ИС проводится Администратор ИБ ИС Министерства в следующих случаях:

прекращения служебного контракта с государственным гражданским служащим Министерства, освобождения его от замещаемой должности гражданской службы и увольнения с гражданской службы;

прекращения действия трудового договора с работником Министерства, замещающего должность, не являющиеся должностями государственной гражданской службы;

прекращения действия трудового договора с работником подведомственной организации.

В данном случае внеплановая смена личного пароля или удаление учётной записи ИС производится немедленно после окончания последнего сеанса работы данного пользователя с ИС.

2.3. Внеплановая полная смена паролей всех пользователей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри Министерства и другие обстоятельства) Администратора ИБ ИС Министерства или специалистов, которым по роду работы были предоставлены полномочия по управлению парольной защитой подсистем автоматизированной системы.

2.4. В случае компрометации личного пароля работника Министерства или подведомственной организации ИС или Устройства проводится внеплановая смена пароля в зависимости от полномочий владельца скомпрометированного пароля.

2.5. Повседневный контроль за действиями работников Министерства и подведомственной организации, обслуживающего персонала ИС и Устройств при работе с паролями, соблюдением порядка их смены, хранения и использования возлагается на Администратора ИБ ИС Министерства.

2.6. Работникам Министерства и подведомственной организации запрещается:

сообщать свой персональный пароль другим лицам или записывать его на материальных носителях, доступных для других лиц (кроме предусмотренных случаев сохранения паролей ключевых учётных записей владельцем информационного актива);

сохранять пароль в программно-технических средствах в открытом виде или использовать средства его автоматического ввода;

использовать легко угадываемый алгоритм смены пароля (например, F%1hTR8 -* F%2hTR8 -> F%3hTR8, или F%1hTR8 -* Fl%hTR8 -* F1h%TR8 и др.);

использовать учётные записи других лиц;

использовать вне Министерства и подведомственной организации пароли, совпадающие с паролями доступа к его автоматизированному рабочему месту;

использовать в качестве паролей примеры, приведенные в Инструкции.

2.7. По решению Администратора ИБ ИС Министерства может применяться резервирование некоторых паролей, таких, как пароли администраторов ИС, пароли ответственных должностных лиц, пароли отдельных пользователей, выполняющих важные функции, пароли, обеспечивающие работу отдельных сетевых сервисов.

2.8. Для резервирования пароля выполняются следующие действия:

пароль записывается на лист бумаги;

лист с записью пароля вкладывается владельцем в конверт, который не должен допускать просмотр записи пароля на просвет. Если конверт недостаточно плотный, в него может быть вложен лист темной бумаги. Конверт заклеивается, при необходимости (для особо важных паролей) опечатывается;

на конверте указывается должность, фамилия и инициалы владельца пароля, наименование информационного средства, которое защищается этим паролем, текущие дату и время, при необходимости другие данные, и заверяет запись личной подписью;

конверт хранится у Администратора ИБ ИС Министерства.

Конверты с паролями хранятся в сейфе Администратора ИБ ИС Министерства. Ответственный за хранение не реже чем один раз в месяц проверяет их наличие по Журналу учёта паролей в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (далее – Журнал учёта паролей) согласно приложению.

При замене пароля конверт передается владельцу пароля, который уничтожает лист с резервным паролем, о чем делается запись в Журнале учёта

паролей. Новый резервный пароль подготавливает Администратора ИБ ИС Министерства к хранению в соответствии с вышеуказанными требованиями. Новый конверт учитывается в Журнале учёта паролей отдельной позицией.

2.9. Вскрытие конверта с паролем производится по решению Администратора ИБ ИС Министерства в случае необходимости использования прав доступа его владельца в отсутствие самого владельца. Для вскрытия конверта назначается комиссия не менее чем из трех работников структурного подразделения Министерства и подведомственной организации. О вскрытии конверта комиссией составляется акт, который по окончании работы комиссии хранится в деле структурного подразделения.

При появлении владельца пароля после факта вскрытия конверта пароль заменяется на новый и вновь сохраняется его копия, как описано выше.

2.10. В зависимости от критичности информационно-технологического актива его владельцем могут быть установлены более высокие требования к сложности пароля и периодичности смены.

ПРИЛОЖЕНИЕ
к Инструкции по организации
парольной защиты при работе
с информационными системами
и устройствами в Министерстве
агропромышленного комплекса
и развития сельских территорий
Ульяновской области
и подведомственной ему организации

ЖУРНАЛ
учёта паролей в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

№ п/п	ФИО владельца (работника)	Должность	Логин (имя пользователя)	Дата генерации пароля	ФИО, выдавшего пароль	Первичный пароль
1	2	3	4	5	6	7

ПРИЛОЖЕНИЕ № 11

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 371

ИНСТРУКЦИЯ
по антивирусной защите информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области

1. Общие положения

1.1. Инструкция по антивирусной защите информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Инструкция) определяет требования к организации защиты информационных систем (далее - ИС) и информационных ресурсов (далее - ИР) Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее – Министерство) от разрушающего воздействия компьютерных вирусов и устанавливает ответственность руководителей и работников структурных подразделений Министерства и подведомственной ему организации (далее – подведомственная организация), эксплуатирующих и сопровождающих ИС Министерства, за их выполнение.

1.2. К использованию в Министерстве и подведомственной организации допускаются только лицензионные и сертифицированные антивирусные средства.

1.3. Изменение используемого антивирусного средства необходимо согласовать с Администратором информационной безопасности информационных систем (далее – Администратор ИБ ИС) Министерства.

1.4. Установка средств антивирусного контроля на рабочих станциях и серверах ИС осуществляется Администратором ИБ ИС Министерства в соответствии с Порядком технического обслуживания, ремонта, модернизации технических и программных средств, входящих в состав информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области.

1.5. Настройка параметров средств антивирусного контроля осуществляется Администратором ИБ ИС Министерства в соответствии руководствами по применению конкретных антивирусных средств.

2. Применение средств антивирусного контроля

2.1. Ежедневно в начале работы при загрузке компьютера в автоматическом режиме должно проводиться обновление антивирусных баз через информационно-телекоммуникационную сеть «Интернет» с сайта разработчика антивирусных средств или иным доступным способом.

2.2. На всех включенных рабочих станциях должен работать в фоновом режиме Антивирус монитор.

2.3. Обязательному антивирусному контролю подлежит любая информация (текстовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам, а также информация на съёмных носителях (магнитных дисках, лентах, CD-ROM и т.п.).

Разархивирование и контроль входящей информации необходимо проводить непосредственно после её приёма.

Возможно применение другого способа антивирусного контроля входящей информации, обеспечивающего аналогичный уровень эффективности контроля. Контроль исходящей информации необходимо проводить непосредственно перед архивированием и отправкой (записью на съёмный носитель).

Файлы, помещаемые в электронный архив должны в обязательном порядке проходить антивирусный контроль.

2.4. Периодические проверки электронных архивов на серверах должны проводиться не реже одного раза в месяц Администратором ИБ ИС Министерства.

2.5. Устанавливаемое (изменяемое) программное обеспечение (далее - ПО) должно быть предварительно проверено Администратором ИБ ИС Министерства на отсутствие программ вирусов и других вредоносных модулей.

Непосредственно после установки (изменения) ПО рабочих станций и серверов ИС должна быть выполнена антивирусная проверка:

на защищаемых серверах и автоматизированных рабочих местах - Администратором ИБ ИС Министерства;

на других серверах и автоматизированных рабочих местах, не требующих защиты, - лицом, установившим (изменившим) ПО.

2.6. 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.) работник Министерства или подведомственной организации самостоятельно должен провести антивирусный контроль своей рабочей станции антивирусным сканером. При необходимости – привлечь Администратора ИБ ИС Министерства для определения ими факта наличия или отсутствия компьютерного вируса.

2.7. В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов работник Министерства или подведомственной организации обязан:

приостановить работу;

немедленно поставить в известность о факте обнаружения заражённых вирусом файлов Администратора ИБ ИС Министерства, владельца заражённых файлов, а также работников Министерства и подведомственной организации, использующих эти файлы в работе;

совместно с владельцем заражённых вирусом файлов провести анализ необходимости дальнейшего их использования;

провести лечение или уничтожение заражённых файлов.

3. Ответственность

3.1. Ответственность за организацию антивирусного контроля в подразделении, эксплуатирующем ИС, в соответствии с требованиями настоящей Инструкции возлагается на Администратора ИБ ИС Министерства.

3.2. Ответственность за проведение мероприятий антивирусного контроля и соблюдение требований настоящей Инструкции возлагается на всех работников Министерства и подведомственной организации, являющихся пользователями ИС.

3.3. Периодический контроль за состоянием антивирусной защиты ИС и ИР Министерства, а также за соблюдением установленного порядка антивирусного контроля и выполнением требований настоящей Инструкции работниками Министерства и подведомственной организации осуществляется Администратором ИБ ИС Министерства.

ПРИЛОЖЕНИЕ № 12

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 371

ИНСТРУКЦИЯ
по резервному копированию данных информационных систем в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

1. Общие положения

1.1. Инструкция по резервному копированию данных информационных систем в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (далее - Инструкция) регламентирует порядок использования систем резервного копирования, архивирования и восстановления информации в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и подведомственной ему организации (далее – подведомственная организация) в целях превентивная защита элементов информационных систем (далее – ИС) Министерства от потери защищаемых информационных ресурсов.

1.2. Защита резервируемой информации в ИС Министерства обеспечивается применением мер защиты информации от неправомерного доступа, уничтожения или модифицирования, определенных в проектной и организационно-распорядительной документации по защите информации в Министерстве и подведомственной организации.

1.3. В ИС Министерства обеспечивается регистрация событий, связанных с резервным копированием информации на резервные машинные носители информации и восстановлением информации с резервных машинных носителей информации.

1.4. Администратор информационной безопасности информационных систем Министерства (далее – Администратор ИБ ИС Министерства) осуществляет не реже одного раза в три месяца проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий.

1.5. Резервное копирование и хранение данных должно осуществляться на периодической основе:

для обрабатываемой информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, – не реже раза в неделю;

для технологической информации – не реже раза в месяц;

эталонных копий программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС Министерства – не реже раза в месяц, и каждый раз при внесении изменений в эталонные копии (выход новых версий);

для записей регистрации (аудита) – не реже одного раза в неделю.

2. Методы резервного копирования

2.1. При выполнении операции «Incremental Backup» производится резервное копирование файлов, изменившихся со времени последнего выполнения операции «Incremental Backup» или «Full Backup».

2.2. При выполнении операции «Full Backup» производится полное резервное копирование информационного ресурса.

3. Порядок хранения носителей резервных копий

3.1. Носители, на которые произведено резервное копирование, должны быть пронумерованы: номером носителя, датой проведения резервного копирования.

3.2. Хранение (размещение) резервных копий информации должно осуществляться на отдельных (размещенных вне ИС) средствах хранения резервных копий и в помещениях, специально предназначенных для хранения резервных копий информации, которые исключают воздействие внешних факторов на хранимую информацию.

3.3. Носители должны храниться не менее года для возможности восстановления данных.

4. Порядок восстановления информации

4.1. Восстановление информации из резервных копий производится Администратором ИБ ИС Министерства на основании согласованной заявки.

4.2. Место расположения восстанавливаемой информации определяется Администратором ИБ ИС Министерства и согласовывается с сотрудником Министерства или подведомственной организации, подавшим заявку, в рабочем порядке.

4.3. Восстановление информации с резервных машинных носителей информации (резервных копий) предусматривает определение времени, в течение которого должно быть обеспечено восстановление информации и обеспечивающего требуемые условия непрерывности функционирования ИС Министерства и доступности информации:

для обрабатываемых персональных данных – не более 6 часов;

для технологической информации – не более 24 часов;

для эталонных копий программного обеспечения (операционные системы, штатное и специальное программное обеспечение, программные средства защиты), с которых осуществляется их установка на элементы ИС Министерства, – не более 24 часов;

для записей регистрации (аудита) – не более 48 часов.

ПРИЛОЖЕНИЕ № 13

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

от 29.05.2020 № 371

ИНСТРУКЦИЯ
по защите информации от утечки по техническим каналам в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

1. Инструкция по защите информации от утечки по техническим каналам в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации (далее - Инструкция) определяет основные меры по защите информации от утечки по техническим каналам в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство) и подведомственной ему организации (далее – подведомственная организация).

2. Для целей настоящей Инструкции используются следующие понятия:

Технический канал утечки информации (далее - ТКУИ) – это совокупность объекта разведки, технического средства разведки (далее - ТСР), с помощью которого добывается информация об объекте, и физической среды в которой распространяется информационный сигнал. Под ТКУИ также понимают способ получения с помощью ТСР разведывательной информации об объекте.

Разведывательная информация – это сведения или совокупность данных об объектах разведки независимо от формы их представления.

3. Меры защиты информации от утечки по техническим каналам.

Допуск пользователей для работы в информационных системах (далее - ИС) Министерства осуществляется в соответствии со списком лиц, допущенных к работе в автоматизированной системе. Для работы в ИС каждый работник должен получить соответствующий доступ, под которым понимается получение каждым работником Министерства и подведомственной организации только письменного разрешения заместителя Председателя Правительства Ульяновской области – Министра агропромышленного комплекса и развития сельских территорий Ульяновской области (далее — Министр) или ответственного должностного лица, уполномоченного соответствующим распоряжением Министерства, на право работы с информацией с учётом его служебных обязанностей.

4. Работник имеет право в отведенное ему время решать поставленные задачи в соответствии с полномочиями доступа к ресурсам ИС, присвоенными

Администратором информационной безопасности информационных систем Министерства (далее – Администратор ИБ ИС Министерства) данному работнику Министерства или подведомственной организации. При этом для хранения файлов, содержащих персональные данные, разрешается использовать только специально выделенные каталоги, а также соответствующим образом учтённые внешние носители.

5. Вход работника Министерства или подведомственной организации в систему осуществляется на основе ввода (по запросу системы) имени, присвоенного для регистрации Администратором ИБ ИС Министерства, и ввода пароля, требования к которому установлены в Инструкции по организации парольной защиты при работе с информационными системами и устройствами в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации.

6. При работе с отчуждаемыми носителями информации работник Министерства или подведомственной организации каждый раз перед началом работы обязан проверить их на наличие вирусов с использованием штатных антивирусных программ, установленных в автоматизированной системе, в соответствии с Инструкцией по антивирусной защите информационных систем и информационных ресурсов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области В случае обнаружения вирусов на внешнем носителе работник Министерства или подведомственной организации обязан предпринять меры по устранению данного инцидента, либо сообщить Администратору ИБ ИС Министерства. В процессе работы работник Министерства или подведомственной организации обязан завершать сеанс и блокировать систему, временно покидая своё автоматизированное рабочее место.

7. На автоматизированном рабочем месте сотрудника Министерства или подведомственной организации установлены специальные средства защиты, предотвращающие вторжение из внешних источников.

8. На сервере Министерства установлены специализированные программные средства защиты информации и предотвращения угроз вторжения и предотвращения разведывательных действий со стороны потенциального злоумышленника.

9. По всем возникающим вопросам при работе в ИС Министерства или возникновению внештатных ситуаций, необходимо обращаться к Администратору ИБ ИС Министерства.

ПРИЛОЖЕНИЕ № 14

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области
№ 371 от 29.05.2020

СПИСОК

помещений, выделенных для установки сертифицированных средств криптографической защиты информации и хранения ключевых документов к ним, съёмных носителей электронной подписи, а также обработки персональных данных в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

№ п/п	Ответственные подразделение	Номер кабинета	Обработка персональных данных	Обработка средств криптографической защиты (СКЗИ)	
				Использование СКЗИ и ключевых документов	Хранение электронной подписи
1	Департамент финансов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области (далее - Министерство)	40	-	-	+
2	Департамент финансов Министерства	39	-	+	+
3	Департамент финансов Министерства	35	+	-	-
4	Отдел обеспечения деятельности областного государственного бюджетного учреждения «Агентство по развитию сельских территорий Ульяновской области» (далее - Агентство)	24	+	+	+
5	Отдел обеспечения деятельности областного государственного бюджетного учреждения Агентства	22	+	-	-
6	Отдел информационных технологий и защиты информации Агентства	12	-	+	+

ПРИЛОЖЕНИЕ № 15

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

№ 371 от 29.05.2020

ЖУРНАЛ
учёта опечатывания помещений, где размещены средства криптографической защиты информации, используемые Министерством агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

№ п/п	Дата	Время		Номер кабинета	ФИО ответственного сотрудника	Должность ответственного сотрудника	Подпись ответственного сотрудника
		Снятие печати	Опечатывание				
1	2	3	4	5	6	7	8

ПРИЛОЖЕНИЕ № 16

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

№ 371 от 29.05. 2020

ЖУРНАЛ
технический (аппаратный) Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

N п/п	Дата	Тип и серийные номера используемых СКЗИ	Записи по обслуживанию СКЗИ	Используемые криптоключи			Отметка об уничтожении (стирании)		Примечание
				Тип ключевого документа	Серийный, криптографический номер и номер экземпляра ключевого документа	Номер разового ключевого носителя или зоны СКЗИ, в которую введены криптоключи	Дата	Подпись пользователя СКЗИ	
1	2	3	4	5	6	7	8	9	10

ПРИЛОЖЕНИЕ № 17

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

№ 371 от 29.05. 2020

ЖУРНАЛ
учёта носителей персональных данных, обрабатываемых в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации

№ п/п	Регистрационный номер	Дата учёта	Тип/ёмкость носителя	Серийный номер	Отметка о постановке на учёт (ФИО ответственного сотрудника, подпись, дата)	Отметка о снятии с учёта (ФИО ответственного сотрудника, подпись, дата)	Местоположение носителя	Сведения об уничтожении носителя/стирании
1	2	3	4	5	6	7	8	9

ПРИЛОЖЕНИЕ № 18

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

№ 371 от 29.05.2020

ЖУРНАЛ
учёта работ в серверном помещении Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области

№ п/п	Дата	Время входа/выхода	Проведённые работы	ФИО ответственного сотрудника	Должность ответственного сотрудника	Подпись ответственного сотрудника
1	2	3	4	5	6	7

ПРИЛОЖЕНИЕ № 19

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

№ 371 от 29.05.2020

ЖУРНАЛ
учёта проверок в области информационных технологий и защиты информации
в Министерстве агропромышленного комплекса и развития сельских территорий Ульяновской области
и подведомственной ему организации

№ п/п	Дата проверки	Тема проверки	Результат проверки	Проверяющий	Подпись проверяющего	Ответственный сотрудник	Подпись ответственного сотрудника
1	2	3	4	5	6	7	8

ПРИЛОЖЕНИЕ № 20

к распоряжению Министерства
агропромышленного комплекса
и развития сельских территорий
Ульяновской области

№ 371 от 29.05.2020

ЖУРНАЛ
учёта журналов Министерства агропромышленного комплекса и развития сельских территорий Ульяновской области и подведомственной ему организации в рамках организации защиты информации

№ п/п	Номер журнала	Наименование журнала	Дата утверждения журнала	ФИО ответственного сотрудника за ведение журнала	Должность ответственного сотрудника за ведение журнала	Подпись ответственного сотрудника за ведение журнала
1	2	3	4	5	6	7