Приложение к приказу
ФГБУ «РосАПКимущество»
от «03 » апреля № 26

Политика информационной безопасности в ФГБУ «РосАПКимущество»

1. Общие положения

1.1. Настоящая Политика информационной безопасности в ФГБУ «РосАПКимущество» (далее соответственно – Политика, Учреждение) разработана в соответствии с положениями:

Конституции Российской Федерации;

Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 27033-1-2011 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции», утвержденного приказом Федерального агентства по техническому регулированию и метрологии от 1 декабря 2011 г. № 683-ст.

1.1.1. Понятия и термины, используемые в информационной безопасности:

Администраторы системы, обрабатывающей информацию в Учреждении – работники отдела информационных технологий и защиты информации;

информация – сведения (сообщения, данные) независимо от формы их представления;

информационные технологии – процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов;

информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств;

информационные ресурсы – электронные документы, предназначенные для использования в Учреждении;

информационно-телекоммуникационная сеть – технологическая система, предназначенная для передачи по линиям связи информации, доступ к которой осуществляется с использованием средств вычислительной техники;

обладатель информации – лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

доступ к информации – возможность получения информации и ее использования;

конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя. Перечень конфиденциальной информации Учреждения установлен согласно приложению № 1 к настоящей Политике;

предоставление информации – действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц;

распространение информации – действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

электронное сообщение – информация, переданная или полученная пользователем информационно-телекоммуникационной сети;

документированная информация – зафиксированная на материальном носителе путем документирования информация с реквизитами, позволяющими определить такую информацию или в установленных законодательством Российской Федерации случаях ее материальный носитель;

электронный документ – документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин, а также для передачи по информационно-телекоммуникационным сетям или обработки в информационных системах;

оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных;

персональные данные – любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);

служебная информация ограниченного распространения – несекретная информация, касающаяся деятельности Министерства сельского хозяйства Российской Федерации (далее – Минсельхоз России), а также подведомственных Минсельхозу России организаций, ограничение на распространение которой диктуется служебной необходимостью. На документах (в необходимых случаях – и на их проектах), содержащих служебную информацию ограниченного распространения, проставляется пометка «Для служебного пользования». Учет таких документов осуществляется в Учреждении в Журнале учета документов ограниченного распространения по форме согласно приложению № 2 к настоящей Политике.

1.1.2. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен.

Общедоступная информация может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации.

Обладатель информации, ставшей общедоступной по его решению, вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации.

Информация, размещаемая ее обладателями в сети «Интернет» в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования, является общедоступной информацией, размещаемой в форме открытых данных.

В случае, если размещение информации в форме открытых данных может повлечь за собой нарушение прав обладателей информации, доступ к которой ограничен в соответствии с федеральными законами, или нарушение прав субъектов персональных данных, размещение указанной информации в форме открытых данных должно быть прекращено по решению суда.

В случае, если размещение информации в форме открытых данных осуществляется с нарушением требований Федерального закона от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (далее – Федеральный закон № 152-ФЗ), размещение информации в форме открытых данных должно быть приостановлено или прекращено по требованию уполномоченного органа по защите прав субъектов персональных данных.

1.2. Политика информационной безопасности представляет собой совокупность положений, правил, требований и принятых решений, определяющих порядок доступа к информационным ресурсам Учреждения, основные направления и способы защиты информации Учреждения.

1.3. Основными целями Политики информационной безопасности Учреждения являются:

защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба;

обеспечение целостности и конфиденциальности информации;

обеспечение соблюдения требований законодательства, локальных нормативных актов Учреждения и общей политики безопасности.

1.4. Основными задачами Политики информационной безопасности Учреждения являются:

доступность обрабатываемой информации;

защита информации от несанкционированного доступа к ней посторонних лиц, от утечки по техническим каналам, от специальных воздействий на информацию в целях её блокирования, уничтожения, искажения;

контроль целостности и аутентичности (подтверждение авторства)

информации, хранимой, обрабатываемой и передаваемой по каналам связи Учреждения;

обеспечение конфиденциальности определенной части информации, хранимой, обрабатываемой и передаваемой по каналам связи Учреждения;

оценка рисков информационной безопасности.

1.5. Защите подлежит вся принимаемая, передаваемая, обрабатываемая и хранимая информация содержащая:

сведения, составляющие служебную информацию, доступ к которым ограничен Учреждением, как собственником информации, в соответствии с положениями предоставленными Федеральным законом от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» персональные данные, доступ к которым ограничен в соответствии с Федеральным законом № 152-ФЗ;

открытые сведения, в части обеспечения доступности и целостности информации.

1.6. Основными способами защиты информационных ресурсов Учреждения являются:

оценка рисков сетевой безопасности;

мониторинг информационной безопасности;

системный аудит;

антивирусный контроль;

анализ инцидентов.

1.7. Основными средствами защиты информационных ресурсов Учреждения являются:

Криптографические программные средства: «криптоПро CSP», «континент TLS»;

встроенные средства контроля событий безопасности.

К программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры, относятся средства защиты информации, в том числе средства защиты информации от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение), межсетевые экраны, средства антивирусной защиты, средства (системы) контроля (анализа) защищенности, средства управления событиями безопасности, средства защиты каналов передачи данных.

средства разграничения доступа к ресурсам автоматизированной системы: «контроллер домена DC»;

средства идентификации и аутентификации пользователей: «контроллер домена DC»;

технические средства защиты: программное обеспечение антивирус «Kaspersky Endpoint Security» (расширенный), встроенный межсетевой экран

роутера.

1.8. Политика информационной безопасности утверждается директором Учреждения и доводится до сведения всех работников Учреждения и соответствующих сторонних организаций при необходимости.

1.9. Основные положения и требования настоящей Политики распространяются на все структурные подразделения Учреждения.

2. Субъекты правоотношений, связанных с использованием информации и обеспечением ее безопасности

2.1. К субъектам правоотношений, связанных с использованием информационных ресурсов Учреждения и обеспечением их безопасности (далее – субъекты правоотношений), относятся:

Учреждение как собственник информационных ресурсов;

директор и его заместители;

помощник директора;

работники Учреждения как пользователи информацией в соответствии с возложенными на них трудовыми обязанностями;

работники Учреждения в соответствии с приказом директора;

отдел информационных технологий и защиты информации Учреждения, обеспечивающий эксплуатацию информационных ресурсов;

отдел ведения реестра РФС АПК;

бухгалтерия;

кадровый работник;

иные пользователи (физические и юридические лица), информация о которых обрабатывается, накапливается и хранится в Учреждении (далее – пользователи).

2.2. Доступ к информационным ресурсам Учреждения имеют работники, установленные приказом директора Учреждения.

Уровень доступа к информационным ресурсам Учреждения определяется для каждого работника индивидуально с соблюдением следующих требований:

каждый работник имеет доступ только к той информации, которая необходима ему для выполнения должностных обязанностей;

непосредственный руководитель работника имеет право на просмотр служебной информации, используемой работником.

В процессе использования информационных ресурсов Учреждения работники обязаны соблюдать следующие требования:

не устанавливать самостоятельно дополнительное программное обеспечение и не запускать программы, скрипты на рабочем месте работника;

не переходить по подозрительным ссылкам в письмах из неизвестных источников;

не использовать флеш накопители, материальные носители ключей

электронной цифровой подписи и внешние накопители данных, не являющиеся имуществом Учреждения;

не использовать служебные персональные компьютеры для посещения ресурсов, не имеющих отношения к исполнению служебных обязанностей работника;

не передавать третьим лицам учетные данные, выданные работнику администратором сети.

2.3. Все работники должны быть ознакомлены персонально с локальными нормативными актами и организационно-распорядительными документами по защите информации, должны знать и неукоснительно выполнять технологические инструкции и общие обязанности по обеспечению безопасности информации.

Каждый работник при приеме на работу подписывает обязательство о соблюдении требований по сохранению конфиденциальной информации и ответственности за их нарушение, а также о выполнении правил работы с информацией.

Все работники, допущенные к работе с информацией Учреждения, в том числе персональными данными, несут персональную ответственность за нарушение правил ее использования, передачи, хранения, а также требований по сохранению информации.

2.4. Доступ к информационным ресурсам Учреждения имеют все пользователи в зависимости от привилегий и политики доступа к данным Учреждения.

Для пользователей разрабатывается инструкция о порядке использования информационных ресурсов Учреждения, включающая требования по обеспечению безопасности информации.

До предоставления доступа к информационным ресурсам Учреждения пользователи должны быть ознакомлены с перечнем конфиденциальной информации и своим уровнем полномочий, а также организационно-распорядительной, локально-нормативной, технической и эксплуатационной документацией, определяющей требования и порядок обработки такой информации.

Пользователи, допущенные к работе с информационными ресурсами Учреждения, несут ответственность за нарушение правил ее использования, передачи, хранения, а также требований по сохранению конфиденциальной информации.

3. Угрозы безопасности информации и их источники

3.1. Угрозы безопасности информации, с которыми сталкивается Учреждение, могут быть связаны с проблемами:

несанкционированного доступа к информации;

несанкционированной передачи информации;

внесения вредоносной программы, отказа от факта приема или источника информации;

отказа в обслуживании и недоступности информации или услуг.

3.2. Указанные угрозы могут быть связаны с утратой:

конфиденциальности информации и программы (в сетях и системах, соединенных с сетями);

целостности информации и программы (в сетях и системах, соединенных с сетями);

доступности информации и сетевых ресурсов;

неотрекаемости сетевых транзакций (обязательств);

подотчетности сетевых транзакций;

подлинности информации (а также аутентичности сетевых пользователей и администраторов);

достоверности информации и программы (в сетях и системах, соединенных с сетями);

способности контролировать несанкционированное использование и эксплуатацию сетевых ресурсов, включая осуществление контроля в контексте политики безопасности Учреждения;

способности контролировать злоупотребление санкционированным доступом.

3.3. Основными источниками угроз безопасности информации являются:

антропогенные источники – умышленные или случайные действия физических лиц (как работников Учреждения, так и посторонних лиц), которые могут привести к нарушению безопасности информации;

техногенные источники – нарушения деятельности технических средств, сбои программного обеспечения, приводящие к рискам утраты информации/несанкционированного доступа к ней 3-х лиц;

стихийные источники – стихийные бедствия или другие обстоятельства природного характера. Такие источники угроз не поддаются прогнозированию в долгосрочной перспективе и, как правило, являются внешними по отношению к защищаемому объекту.

4. Мониторинг информационной безопасности

4.1. Мониторинг работоспособности аппаратных компонентов автоматизированных систем, обрабатывающих информацию, осуществляется в процессе их администрирования и при проведении работ по техническому обслуживанию оборудования.

Наиболее существенные компоненты системы, имеющие встроенные средства контроля работоспособности (серверы, активное сетевое оборудование), должны контролироваться постоянно в рамках работы администраторов соответствующих систем.

4.2. Мониторинг парольной защиты и контроль надежности пользовательских паролей предусматривают установление сроков действия паролей один раз в год.

4.3. Мониторинг целостности программного обеспечения включает следующие действия:

проверка контрольных сумм и цифровых подписей каталогов и файлов сертифицированных программных средств при загрузке операционной системы;

обнаружение дубликатов идентификаторов пользователей;

восстановление системных файлов администраторами систем с резервных копий.

4.4. Мониторинг попыток несанкционированного доступа осуществляется с использованием средств операционной системы и специальных программных средств и предусматривает:

фиксацию неудачных попыток входа в систему в системном журнале;

протоколирование работы сетевых сервисов;

выявление фактов сканирования определенного диапазона сетевых портов в короткие промежутки времени с целью обнаружения сетевых анализаторов, изучающих систему и выявляющих ее уязвимости.

4.5. Мониторинг производительности автоматизированных систем, обрабатывающих информацию, производится по обращениям пользователей в ходе администрирования систем и проведения профилактических работ для выявления попыток несанкционированного доступа, повлекших существенное уменьшение производительности систем.

5. Антивирусный контроль

5.1. Для защиты серверов и рабочих станций необходимо использовать антивирусные программы:

резидентные антивирусные мониторы, контролирующие подозрительные действия программ;

утилиты для обнаружения и анализа новых вирусов.

5.2. К использованию допускаются только лицензионные средства защиты от вредоносных программ и вирусов или сертифицированные свободно распространяемые антивирусные средства.

5.3. При подозрении на наличие не выявленных установленными средствами защиты заражений следует использовать операционную систему, загружающуюся со сменного носителя с другими антивирусными средствами.

5.4. Установка и настройка средств защиты от вредоносных программ и вирусов на рабочих станциях и серверах автоматизированных систем, обрабатывающих персональные данные, осуществляется администраторами соответствующих систем в соответствии с руководствами по установке приобретенных средств защиты.

5.5. Устанавливаемое (изменяемое) программное обеспечение должно быть предварительно проверено администратором системы на отсутствие вредоносных программ и компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения рабочей станции должна быть выполнена антивирусная проверка.

5.6. Запуск антивирусных программ должен осуществляться автоматически по заданию, централизованно созданному с использованием планировщика задач (входящим в поставку операционной системы либо поставляемым вместе с антивирусными программами).

5.7. Антивирусный контроль рабочих станций должен проводиться ежедневно в автоматическом режиме. Если проверка всех файлов на дисках рабочих станций занимает неприемлемо большое время, то допускается проводить выборочную проверку загрузочных областей дисков, оперативной памяти, критически важных инсталлированных файлов операционной системы и загружаемых файлов по сети или с внешних носителей. В этом случае полная проверка должна осуществляться не реже одного раза в неделю в период неактивности пользователя. Пользователям рекомендуется осуществлять полную проверку во время перерыва на обед путем перевода рабочей станции в соответствующий автоматический режим функционирования в запертом помещении.

5.8. Обязательному антивирусному контролю подлежит любая информация (исполняемые файлы, текстовые файлы любых форматов, файлы данных), получаемая пользователем по сети или загружаемая со съемных носителей (магнитных дисков, оптических дисков, флеш-накопителей и т. п.). Контроль информации должен проводиться антивирусными средствами в процессе или сразу после ее загрузки на рабочую станцию пользователя. Файлы, помещаемые в электронный архив, должны в обязательном порядке проходить антивирусный контроль.

5.9. Устанавливаемое (изменяемое) на серверы программное обеспечение должно быть предварительно проверено администратором системы на отсутствие компьютерных вирусов и вредоносных программ. Непосредственно после установки (изменения) программного обеспечения сервера должна быть выполнена антивирусная проверка.

5.10. На серверах систем, обрабатывающих персональные данные, необходимо применять специальное антивирусное программное обеспечение, позволяющее:

осуществлять антивирусную проверку файлов в момент попытки записи файла на сервер;

проверять каталоги и файлы по расписанию с учетом нагрузки на сервер.

5.11. На серверах электронной почты необходимо применять антивирусное программное обеспечение, обеспечивающее проверку всех входящих сообщений. В случае если проверка входящего сообщения на почтовом сервере показала наличие в нем вируса или вредоносного кода, отправка данного сообщения должна

блокироваться. При этом должно осуществляться автоматическое оповещение администратора почтового сервера, отправителя сообщения и адресата.

5.12. На всех рабочих станциях и серверах необходимо организовать регулярное обновление антивирусных баз.

5.13. Администраторы систем должны проводить регулярные проверки протоколов работы антивирусных программ с целью выявления пользователей и каналов, через которые распространяются вирусы.

5.14. При обнаружении зараженных вирусом файлов администратор системы должен выполнить следующие действия:

отключить от компьютерной сети рабочие станции, представляющие вирусную опасность, до полного выяснения каналов проникновения вирусов и их уничтожения;

немедленно сообщить о факте обнаружения вирусов непосредственному начальнику с указанием предположительного источника (отправителя, владельца и т. д.) зараженного файла, типа зараженного файла, характера содержащейся в файле информации, типа вируса и выполненных антивирусных мероприятий.

6. Анализ инцидентов

6.1. Если администратор системы, обрабатывающей информацию, подозревает или получил сообщение о том, что его система подвергается атаке или уже была скомпрометирована, то он должен установить:

факт попытки несанкционированного доступа (НСД);

продолжается ли НСД в настоящий момент;

кто является источником НСД;

что является объектом НСД;

когда происходила попытка НСД;

как и при каких обстоятельствах была предпринята попытка НСД;

точку входа нарушителя в систему;

была ли попытка НСД успешной;

определить системные ресурсы, безопасность которых была нарушена;

какова мотивация попытки НСД.

6.2. Для выявления попытки НСД необходимо:

установить, какие пользователи в настоящее время работают в системе, на каких рабочих станциях;

выявить подозрительную активность пользователей;

проверить, что все пользователи вошли в систему со своих рабочих мест, и никто из них не работает в системе необычно долго;

проверить, что никто из пользователей не использует подозрительных программ и программ, не относящихся к его области деятельности.

6.3. При анализе системных журналов администратору необходимо произвести

следующие действия:

проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД, включая вход в систему пользователей, которые должны бы были отсутствовать в этот период времени, входы в систему из неожиданных мест, в необычное время и на короткий период времени;

проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;

просмотреть списки команд, выполненных пользователями в рассматриваемый период времени;

проверить наличие исходящих сообщений электронной почты, адресованных подозрительным хостам;

проверить наличие мест в журналах, которые выглядят необычно;

выявить попытки получить полномочия пользователя с расширенным полномочиями;

выявить наличие неудачных попыток входа в систему.

6.4. В ходе анализа журналов активного сетевого оборудования (мостов, переключателей, маршрутизаторов, шлюзов) необходимо:

проверить наличие подозрительных записей системных журналов, сделанных в период предполагаемой попытки НСД;

проверить, не уничтожен ли системный журнал и нет ли в нем пробелов;

проверить наличие мест в журналах, которые выглядят необычно;

выявить попытки изменения таблиц маршрутизации и адресных таблиц;

проверить конфигурацию сетевых устройств с целью определения возможности нахождения в системе программы, просматривающей весь сетевой трафик.

6.5. Для обнаружения в системе следов, оставленных злоумышленником, в виде файлов, вирусов, троянских программ, изменения системной конфигурации необходимо:

составить базовую схему того, как обычно выглядит система;

провести поиск подозрительных файлов, скрытых файлов, имена файлов и каталогов которых обычно используются злоумышленниками;

проверить содержимое системных файлов, которые обычно изменяются злоумышленниками;

проверить целостность системных программ;

проверить систему аутентификации и авторизации.

6.6. В случае заражения значительного количества рабочих станций после устранения его последствий проводится системный аудит.

7. Особенности обеспечения информационной безопасности персональных данных

7.1. В Учреждении выделяются следующие категории персональных данных:

специальные категории персональных данных;

биометрические персональные данные;

общедоступные или обезличенные персональные данные;

персональные данные, которые не могут быть отнесены к специальным категориям персональных данных, к биометрическим персональным данным, к общедоступным или обезличенным персональным данным.

7.2. К персональным данным субъекта относятся:

год и место рождения, гражданство;

прежние фамилия, имя, отчество, дата, место и причина изменения (в случае изменения);

владение иностранными языками и языками народов Российской Федерации;

образование (когда и какие образовательные учреждения закончил, номера дипломов, направление подготовки или специальность по диплому, квалификация по диплому);

послевузовское профессиональное образование (наименование образовательного или научного учреждения, год окончания), ученая степень, ученое звание (когда присвоены, номера дипломов, аттестатов);

государственные награды, иные награды и знаки отличия (кем награжден и когда);

степень родства, фамилии, имена, отчества, даты рождения близких родственников (отца, матери, братьев, сестер и детей), а также мужа (жены);

адрес регистрации и фактического проживания дата регистрации по месту жительства;

паспорт (серия, номер, кем и когда выдан);

свидетельства о государственной регистрации актов гражданского состояния;

номер телефона;

отношение к воинской обязанности, сведения по воинскому учету (для граждан, пребывающих в запасе, и лиц, подлежащих призыву на военную службу);

сведения о трудовом стаже, предыдущих местах работы, доходах с предыдущих мест работы;

информация о приеме, переводе, увольнении и иных событиях, относящихся к трудовой деятельности в Учреждении;

сведения о доходах в ФГБУ «РосАПКимущество»;

идентификационный номер налогоплательщика (при его наличии у работника);

номер страхового свидетельства обязательного пенсионного страхования.

7.3. Все персональные сведения о субъекте персональных данных Работодатель может получить только от него самого либо формирует в процессе работы (информация о событиях, относящихся к трудовой деятельности в Учреждении, сведения о доходах, награды).

7.4. Работодатель обязан сообщить субъекту персональных данных о целях, способах и источниках получения персональных данных, а также о характере подлежащих получению персональных данных и возможных последствиях отказа работника дать письменное согласие на их получение.

7.5. Персональные данные субъекта персональных данных являются конфиденциальной информацией и не могут быть использованы Учреждением или любым иным лицом в личных целях.

7.6. При определении объема и содержания персональных данных Учреждение руководствуется Конституцией Российской Федерации, иными федеральными законами.

7.7. Все документы с персональными данными хранятся способом, исключающим посторонний несанкционированный доступ.

7.8. Право доступа к персональным данным имеют работники, установленные приказом директора.

7.9. Учреждение обязано принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей по защите персональных данных, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним локальными нормативными актами.

Учреждение самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей по защите персональных данных, предусмотренных Федеральным законом № 152-ФЗ и принятыми в соответствии с ним нормативными правовыми актами. К таким мерам могут, в частности, относиться:

назначение ответственного за организацию обработки персональных данных;

принятие актов, определяющих политику Учреждения в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

применение правовых, организационных и технических мер по обеспечению безопасности персональных данных;

осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону № 152-ФЗ и принятым в соответствии с ним локальным нормативным актам, требованиям к защите персональных данных, политике оператора в отношении обработки персональных данных, локальным актам оператора;

оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона № 152-ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом № 152-ФЗ;

ознакомление работников, непосредственно осуществляющих обработку

персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных и (или) обучение указанных работников.

7.10. В случае выявления неправомерной обработки персональных данных при обращении субъекта персональных данных Учреждение осуществляет блокирование неправомерно обрабатываемых персональных данных с момента такого обращения на период проверки.

7.11. В случае выявления неточных персональных данных при обращении субъекта персональных данных Учреждение осуществляет блокирование персональных данных с момента такого обращения на период проверки, если блокирование персональных данных не нарушает права и законные интересы субъекта персональных данных или третьих лиц.

7.12. В случае подтверждения факта неточности персональных данных Учреждение на основании сведений, представленных субъектом персональных данных, или иных необходимых документов уточняет персональные данные в течение семи рабочих дней со дня представления таких сведений и снимает блокирование персональных данных.

7.13. В случае выявления неправомерной обработки персональных данных работников в Учреждении работодатель прекращает неправомерную обработку персональных данных работников в срок, не превышающий трех рабочих дней с даты этого выявления.

7.14. В случае если обеспечить правомерность обработки персональных данных невозможно, Учреждение в срок, не превышающий десяти рабочих дней с даты выявления неправомерной обработки персональных данных, уничтожает такие персональные данные.

7.15. Об устранении допущенных нарушений или об уничтожении персональных данных Учреждение уведомляет субъекта персональных данных.

7.16. В случае достижения цели обработки персональных данных Учреждение прекращает обработку персональных данных и уничтожает персональные данные в срок, не превышающий тридцати дней с даты достижения цели обработки персональных данных.

7.17. В случае отзыва субъектом персональных данных согласия на обработку его персональных данных Учреждение прекращает их обработку и в случае, если сохранение персональных данных более не требуется для целей обработки персональных данных, уничтожает персональные данные в срок, не превышающий тридцати дней с даты поступления указанного отзыва.

7.18. В случае отсутствия возможности уничтожения персональных данных в течение срока, указанного в пунктах 9.13-9.16 настоящей Политики, Учреждение осуществляет блокирование таких персональных данных и обеспечивает

уничтожение персональных данных в срок не более чем шесть месяцев, если иной срок не установлен федеральными законами.

7.19. Лица, виновные в нарушении норм, регулирующих получение, обработку и защиту персональных данных, привлекаются к дисциплинарной и материальной ответственности в порядке, установленном федеральными законами, а также привлекаются к гражданско-правовой, административной и уголовной ответственности в порядке, установленном федеральными законами.

7.20. Моральный вред, причиненный субъекту персональных данных вследствие нарушения его прав, нарушения правил обработки персональных данных, установленных Федеральным законом № 152-ФЗ, а также требований к защите персональных данных, установленных в соответствии с Федеральным законом № 152-ФЗ, подлежит возмещению в соответствии с законодательством Российской Федерации. Возмещение морального вреда осуществляется независимо от возмещения имущественного вреда и понесенных субъектом персональных данных убытков.

8. Порядок обращения с документами, содержащими служебную информацию ограниченного распространения

8.1. Настоящая Политика определяет общий порядок обращения с документами и другими материальными носителями служебной информации ограниченного распространения (фото-, кино-, видео- и аудио-пленки, машинные носители информации) (далее – документами с грифом «ДСП»), содержащими служебную информацию ограниченного распространения, в Учреждении.

Категории должностных лиц Учреждения, имеющие право обрабатывать служебную информацию:

директор, заместители и помощник директора, начальники структурных подразделений Учреждения, главный бухгалтер, кадровый работник, а также иные лица, установленные приказом директора Учреждения.

8.2. К служебной информации ограниченного распространения относится несекретная информация, поступившая из Министерства с грифом «ДСП», подготовленная в ответ Учреждением информация на запросы Министерства с грифом «ДСП», а также иная информация, ограничение на распространение которой диктуется служебной необходимостью.

8.3. Не могут быть отнесены к служебной информации ограниченного распространения:

акты законодательства;

сведения о чрезвычайных ситуациях, опасных природных явлениях и процессах, экологическая, гидрометеорологическая, гидрогеологическая, демографическая, санитарно-эпидемиологическая и другая информация,

необходимая для обеспечения безопасного существования населенных пунктов, граждан, а также производственных объектов;

описание структуры Учреждения, его функций, направлений и форм деятельности, а также его адрес;

порядок рассмотрения заявлений и обращений граждан и юридических лиц;

решения по заявлениям и обращениям граждан и юридических лиц, рассмотренным в установленном порядке;

сведения об исполнении государственного задания;

документы, накапливаемые в открытых фондах, информационных системах, необходимые для реализации прав, свобод и обязанностей граждан.

8.4. Каждый работник Учреждения предупреждается об ответственности за разглашение служебной информации ограниченного распространения, ставшей ему известной в связи с выполнением им своих служебных обязанностей.

8.5. За разглашение служебной информации ограниченного распространения, за нарушение порядка обращения с документами, содержащими такую информацию, ответственные лица могут быть привлечены к дисциплинарной ответственности.

8.6. При работе со служебной информацией ограниченного распространения работники Учреждения обязаны:

хранить в тайне известную им служебную информацию ограниченного распространения, письменно информировать директора о фактах нарушения порядка обращения со служебной информацией ограниченного распространения, о попытках несанкционированного доступа к ней;

строго соблюдать правила пользования документами «ДСП», порядок их учета и хранения, исключать доступ к ним посторонних лиц;

знакомиться только с теми документами «ДСП», к которым получен доступ в силу исполнения прямых служебных обязанностей.

8.7. При работе со служебной информацией ограниченного распространения работникам Учреждения запрещается:

использовать служебную информацию ограниченного распространения при ведении переговоров по телефонной сети, а также с использованием мобильных средств связи;

передавать документы, содержащие служебную информацию ограниченного распространения, в общедоступной переписке;

передавать документы, содержащие служебную информацию ограниченного распространения, по незащищенным каналам связи (факсимильная связь, электронная почта и т.п.);

использовать служебную информацию ограниченного распространения при общении с работниками Учреждения, не имеющими отношения к этим сведениям;

снимать копии с документов, содержащих служебную информацию ограниченного распространения, без разрешения директора Учреждения;

выполнять работы, связанные со служебной информацией ограниченного распространения, на дому, выносить документы и другие носители информации, содержащие данные сведения, из здания Учреждения без разрешения соответствующих должностных лиц.

Обмен документами «ДСП» в электронном виде осуществляется с помощью учтенного USB-носителя.

8.8. Прием, учет (регистрация) документов, содержащих информацию ограниченного распространения, осуществляет помощник директора, лицо, ответственное за делопроизводство.

Документы с пометкой «Для служебного пользования»:

создаются на автоматизированном рабочем месте с закрытым доступом в общую информационную систему Учреждения (локальную сеть);

передаются ответственным лицам под расписку способом, исключающим прочтение посторонними лицами;

пересылаются по почте заказными почтовыми отправлениями либо передаются нарочно;

регистрируются в специальном журнале;

хранятся в металлическом шкафу с запирающим устройством.

8.9. Запрещается сканирование – введение в систему электронного документооборота электронной версии документов с пометкой «Для служебного пользования» с отметкой для всеобщего доступа.

8.10. Уничтожение документов с пометкой «Для служебного пользования», утративших свое практическое значение, производится по акту.

8.11. Содержание помещений, в которых ведется работа и хранятся документы и другие материальные носители, содержащие служебную информацию ограниченного распространения, должно исключать возможность бесконтрольного проникновения в них посторонних лиц и гарантировать сохранность документов.

8.12. Для хранения документов с пометкой «ДСП» помещение снабжается металлическим шкафом с запирающим устройством.

9. Заключительные положения

9.1. Настоящая Политика вступает в силу с момента ее утверждения.

9.2. Настоящая Политика доводится до сведения всех работников Учреждения.

С Политикой информационной безопасности в ФГБУ «РосАПКимущество» ознакомлены:

№ п/п	Ф. И. О. работника	Дата	Подпись
1	2	3	4

Приложение № 1
к Политике информационной безопасности
в ФГБУ «РосАПКимущество»

Перечень
конфиденциальной информации Учреждения

1. Персональные данные работников Учреждения, за исключением сведений, подлежащих распространению в средствах массовой информации.

2. Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами.

3. Сведения, содержащиеся в документах по организации воинского учета и мобилизационной работы.

4. Сведения об организации и состоянии систем безопасности жизнедеятельности, в том числе системы защиты информации.

5. Организация и состояние охраны и пропускного режима.

6. Организация, схемы размещения, возможности и состояние системы охраны техническими средствами, в том числе системы видеонаблюдения, номера электронных ключей (пропуска).

7. Сведения, составляющие материалы служебных расследований, проверок, дознания, следствия, судопроизводства.

8. Ключевая информация, предназначенная для осуществления криптографической защиты информации, сведения о порядке ее использования.

9. Сведения об организации, порядке использования, состоянии, администрировании и резервного копирования защищаемой информации.

10. Организация и состояние систем администрирования, управления доступом.

11. Информация о ходе и результатах выполнения Учреждением государственного задания (материалы проверок, материалы консультаций и т.д.).

12. Сведения об учетных данных ПО в финансово-бухгалтерской деятельности Учреждения, в том числе логин, пароль и ЭЦП (Банк-клиент, 1С, СБИС и иное).

Приложение № 2
к Политике информационной безопасности
в ФГБУ «РосАПКимущество»

ФОРМА

Для служебного пользования
Экз. №_____
ФГБУ «РосАПКимущество»
Наименование структурного подразделения
Дело N 00-00 Том № 0

Журнал

учета документов, содержащих служебную информацию ограниченного распространения
(для служебного пользования)

Начато: 20____ год

Окончено: 20____ год
На _____ листах
Срок хранения: 5 лет
Лицо, ответственное за делопроизводство
_____ФИО:

№ п/п	Дата поступления документа	Номер и дата входящего документа	Краткое содержание документа	Номер и дата исходящего документа	Исполнитель	
1	**2**	**3**	**4**	**5**	**6**	

№ экземп. № копии	Кол-во листов	№ дела	Отметка об уничтожении или передачи в архив (№ и дата акта)	Дата и подпись	
				О получении	О возврате
7	**8**	**9**	**10**	**11**	**12**

Для служебного пользования

Экз.№ _____

ФГБУ «РосАПКимущество»

Наименование структурного подразделения

Дело № 00-00 Том №0

Журнал

учета съемных электронных носителей информации ограниченного распространения (для служебного пользования)

Начато: 20____ год

Окончено: 20____

год

На _____ листах

Срок хранения: 5 лет

Лицо, ответственное за делопроизводство: _____ФИО

№ п/п	Тип носителя, его учетный номер	Кол-во файлов	Роспись в получении	Роспись о сдаче	Отметка об уничтожении, № акта	Примечание
1	**2**	**3**	**4**	**5**	**6**	**7**