ГЕНЕРАЛЬНАЯ
ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ

ПРИКАЗ

24.11.2021 № 701

Москва

Об утверждении Инструкции по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации

В целях надлежащей эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации и безопасного использования в органах прокуратуры Российской Федерации возможностей информационно-телекоммуникационной сети «Интернет», руководствуясь пунктом 1 статьи 17 Федерального закона «О прокуратуре Российской Федерации»,

П Р И К А З Ы В А Ю:

1. Утвердить Инструкцию по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации (далее – Инструкция).

2. Запретить размещение в открытом доступе в информационно-телекоммуникационной сети «Интернет» документов, содержащих служебную информацию, персональные данные и иные сведения конфиденциального характера (за исключением случаев, когда это прямо предусмотрено федеральным законодательством и организационно-распорядительными документами Генеральной прокуратуры Российской Федерации).

3. Заместителю Генерального прокурора Российской Федерации – Главному военному прокурору, ректору Университета прокуратуры Российской Федерации:

разработать и утвердить аналогичные инструкции по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов в органах военной прокуратуры, Университете прокуратуры Российской Федерации соответственно;

определить должностных лиц, ответственных за установку, настройку и сопровождение программного обеспечения, соблюдение требований по обеспечению информационной безопасности, эксплуатацию автоматизированных рабочих мест и иных технических средств, а также за осуществление контроля за действиями пользователей, использованием служебной электронной почты.

4. Возложить на Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации:

контроль за соблюдением в органах и организациях прокуратуры Российской Федерации требований по обеспечению информационной безопасности при работе в информационных системах и информационно-телекоммуникационной сети «Интернет»;

осуществление в структурных подразделениях Генеральной прокуратуры Российской Федерации, дислоцированных в г. Москве, установки, настройки и сопровождения программного обеспечения, контроля за эксплуатацией автоматизированных рабочих мест и иных служебных технических средств, подключенных к информационно-телекоммуникационной сети «Интернет», использованием служебной электронной почты;

организацию предоставления в органах и организациях прокуратуры Российской Федерации возможности использования служебной электронной почты с выделением соответствующих адресов;

обеспечение защищенности программно-технического комплекса, предназначенного для автоматизации деятельности в органах прокуратуры Российской Федерации с доступом к сети «Интернет».

5. Прокурорам субъектов Российской Федерации, приравненным к ним специализированным прокурорам, прокурору комплекса «Байконур» путем издания соответствующих организационно-распорядительных документов определить ответственных работников за соблюдение требований по обеспечению информационной безопасности при работе в информационных системах и в информационно-телекоммуникационной сети «Интернет».

6. Начальникам структурных подразделений Генеральной прокуратуры Российской Федерации по федеральным округам (за исключением управления Генеральной прокуратуры Российской Федерации по Центральному федеральному округу), прокурорам субъектов Российской Федерации, приравненным к ним специализированным прокурорам, прокурору комплекса «Байконур» путем издания соответствующих организационно-распорядительных документов определить работников, осуществляющих установку, настройку и сопровождение программного обеспечения, контроль за эксплуатацией автоматизированных рабочих мест и иных служебных технических средств, подключенных к информационно-телекоммуникационной сети «Интернет», использованием служебной электронной почты.

7. Заместителю Генерального прокурора Российской Федерации – Главному военному прокурору, начальникам структурных подразделений Генеральной прокуратуры Российской Федерации, ректору Университета прокуратуры Российской Федерации, прокурорам субъектов Российской Федерации, приравненным к ним специализированным прокурорам, прокурору комплекса «Байконур»:

обеспечить соблюдение требований настоящего приказа;

в случаях выявления нарушений требований приказа инициировать проведение проверок в соответствии с положениями организационно-распорядительных документов Генеральной прокуратуры Российской Федерации, регламентирующих порядок проведения проверок в отношении работников органов и организаций прокуратуры Российской Федерации, и при необходимости ставить вопрос о привлечении виновных лиц к ответственности;

ежегодно анализировать состояние работы по соблюдению требований приказа. Результаты анализа с информацией о выявленных нарушениях, принятых мерах и указанием проблемных вопросов направлять в Главное управление правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации в срок до 1 февраля;

организовать изучение подчиненными работниками в 30-дневный срок со дня поступления, а также вновь принятыми на службу в органы и организации прокуратуры Российской Федерации работниками в 3-дневный срок со дня фактического начала работы:

Указа Президента Российской Федерации от 17.03.2008 № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена»;

Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

приказа Генерального прокурора Российской Федерации от 31.05.2011 № 153 «Об организации работы по обеспечению доступа к информации о деятельности органов и организаций прокуратуры Российской Федерации»;

приказа Генерального прокурора Российской Федерации от 04.04.2019 № 249 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в органах и организациях прокуратуры Российской Федерации и Перечня сведений, содержащих служебную информацию ограниченного распространения»;

настоящего приказа.

8. Главному управлению правовой статистики и информационных технологий Генеральной прокуратуры Российской Федерации обобщать информацию о соблюдении требований настоящего приказа с последующим ежегодным докладом Генеральному прокурору Российской Федерации в срок до 1 апреля.

9. Признать утратившими силу приказы Генерального прокурора Российской Федерации от 11.09.2002 № 56 «Об утверждении временной инструкции о порядке работы сотрудников Генеральной прокуратуры Российской Федерации в сети «Интернет» и от 08.09.2016 № 565 «Об утверждении и введении в действие Инструкции пользователю служебной ПЭВМ органов и учреждений прокуратуры Российской Федерации».

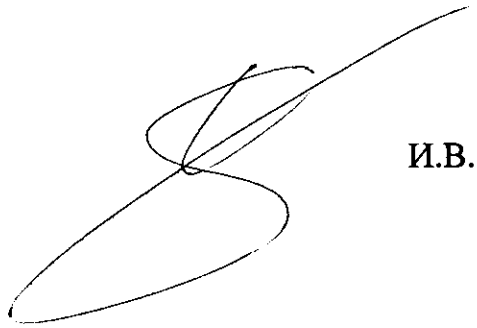
10. Приказ опубликовать в журнале «Законность» и разместить на официальном сайте Генеральной прокуратуры Российской Федерации в информационно-телекоммуникационной сети «Интернет».

11. Контроль за исполнением приказа возложить на заместителей Генерального прокурора Российской Федерации по направлениям деятельности.

Приказ направить заместителям Генерального прокурора Российской Федерации, советникам Генерального прокурора Российской Федерации, старшим помощникам Генерального прокурора Российской Федерации по особым поручениям, помощникам заместителей Генерального прокурора Российской Федерации по особым поручениям, начальникам главных управлений, управлений и отделов Генеральной прокуратуры Российской Федерации, ректору Университета прокуратуры Российской Федерации, прокурорам субъектов Российской Федерации, приравненным к ним специализированным прокурорам и прокурору комплекса «Байконур», которым довести его содержание до сведения подчиненных работников.

Генеральный прокурор
Российской Федерации

действительный государственный
советник юстиции



И.В. Краснов

УТВЕРЖДЕНА

приказом
Генерального прокурора
Российской Федерации
от 24.11.2021 № 701

ИНСТРУКЦИЯ ПО ЭКСПЛУАТАЦИИ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ, ИНФОРМАЦИОННЫХ СИСТЕМ И ИНФОРМАЦИОННЫХ РЕСУРСОВ ОРГАНОВ ПРОКУРАТУРЫ РОССИЙСКОЙ ФЕДЕРАЦИИ

1. Общие положения и область применения

1.1. Инструкция по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации (далее – Инструкция) разработана на основании требований инструкций по эксплуатации технических и программных средств производителя, Федерального закона от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации», постановления Главного государственного санитарного врача Российской Федерации от 02.12.2020 № 40 «Об утверждении санитарных правил СП 2.2.3670-20 «Санитарно-эпидемиологические требования к условиям труда» в целях повышения эффективности данной работы и уровня информационной безопасности.

1.2. Положения Инструкции устанавливают на единой основе в органах прокуратуры Российской Федерации правила использования средств вычислительной техники, информационных систем и информационных ресурсов, обязанности при осуществлении указанной работы и ответственность за несоблюдение правил.

1.3. Настоящая Инструкция распространяется на все виды работ на средствах вычислительной техники и в информационных системах, регламентирует порядок работы в органах прокуратуры Российской Федерации в информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»).

2. Перечень использованных сокращений, единиц и терминов

В настоящей Инструкции используются следующие понятия:

Автоматизированное рабочее место (АРМ) – программно-технический комплекс, предназначенный для автоматизации деятельности

в органах (организациях) прокуратуры Российской Федерации.

«АРМ – Интернет» – служебный персональный компьютер для реализации доступа пользователей к информационным ресурсам сети «Интернет».

Администратор – уполномоченный работник органа (организации) прокуратуры Российской Федерации, осуществляющий установку и обслуживание информационных систем и средств вычислительной техники.

АИК «Надзор-WEB» – автоматизированный информационный комплекс единой системы информационно-документационного обеспечения надзорного производства в органах прокуратуры.

Видео-конференц-связь (ВКС) – телекоммуникационная технология интерактивного взаимодействия трех и более удаленных абонентов, при которой между ними возможен обмен аудио- и видеоинформацией в реальном времени с учетом передачи управляющих данных.

Внешняя почта ИСОП – сервис электронной почты, расположенный в ОС ЕЗСПД и позволяющий обмениваться электронными сообщениями с гражданами и организациями посредством сегмента RSNET сети «Интернет».

Внутренняя почта ИСОП – сервис электронной почты, расположенный в ЗС ЕЗСПД и позволяющий обмениваться электронными сообщениями только внутри органов (организаций) прокуратуры.

ЕЗСПД – единая защищенная сеть передачи данных органов (организаций) прокуратуры Российской Федерации.

Закрытый сегмент ЕЗСПД (ЗС ЕЗСПД) – часть ЕЗСПД, где размещены ресурсы и сервисы органов (организаций) прокуратуры Российской Федерации без возможности выхода в сеть «Интернет».

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

Информационная система (ИС) – совокупность содержащейся в базах данных информации, а также информационных технологий и технических средств, обеспечивающих ее обработку.

Информационный ресурс (ИР) – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах (библиотеках, архивах, фондах, банках данных, других информационных системах).

Информация ограниченного распространения – несекретная информация, касающаяся деятельности органов (организаций) прокуратуры Российской Федерации, ограничения на распространение которой диктуются служебной необходимостью, а также несекретная информация, поступившая в органы (организации) прокуратуры Российской Федерации, доступ к которой ограничен в соответствии с требованиями федерального законодательства.

ИСОП – совокупность информационных систем, ресурсов и сервисов органов (организаций) прокуратуры Российской Федерации, расположенных в

закрытом и открытом сегментах ЕЗСПД.

Ключевой носитель – физический носитель, предназначенный для размещения на нем ключевой информации.

Компрометация – утрата, разглашение учетных данных, доступ к ним или подозрение о возможном несанкционированном доступе постороннего лица к учетным данным или средствам электронной подписи.

Конфиденциальная информация – информация, содержащая персональные данные работников органов (организаций) прокуратуры, а также сведения конфиденциального характера в соответствии с перечнем, утвержденным Указом Президента Российской Федерации от 06.03.1997 № 188.

Локальная вычислительная сеть – совокупность аппаратного и программного обеспечения, позволяющего объединить средства вычислительной техники в единую распределенную систему обработки и хранения информации.

Материально ответственное лицо – уполномоченный работник органа (организации) прокуратуры Российской Федерации, осуществляющий приемку, учет, хранение, выдачу, перемещение материальных средств и ценностей.

Машинный носитель информации (МНИ) – носитель данных, предназначенный для записи и считывания данных (HDD, SSD, USB-флеш-накопитель, DVD (CD) оптический диск), который может быть несъемным (установленный внутри АРМ) и съемным (переносной, временно подключаемый к средствам вычислительной техники через стандартные разъемы).

Несанкционированный доступ – доступ к информации или информационной системе со стороны лиц, не имеющих соответствующего разрешения.

Открытый сегмент ЕЗСПД (ОС ЕЗСПД) – часть ЕЗСПД, предоставляющая доступ к сети «Интернет» через сегмент RSNET.

Подразделение криптографической защиты – структурное подразделение (работник) органа (организации) прокуратуры Российской Федерации, уполномоченное на организацию и обеспечение безопасности хранения, передачи, использования и уничтожения средств криптографической защиты информации, а также осуществляющее мероприятия по криптографической защите информации с применением ключевых документов.

Персональная электронная почта – адрес электронной почты работника органа (организации) прокуратуры Российской Федерации.

Пользователь – работник органа (организации) прокуратуры Российской Федерации, которому в рамках исполнения его служебных обязанностей предоставлен доступ к информационным системам и средствам вычислительной техники.

Посторонняя информация – информация, не имеющая отношения к выполнению служебных обязанностей (не входящее в список разрешенного к использованию в работе программное обеспечение, фильмы, музыка, фотографии, игры и т. д.).

Почта «Интернет» – сервис электронной почты, расположенный за

пределами ЕЗСПД на внешних ресурсах сети «Интернет». Данные почтовых сообщений могут храниться как на территории России, так и за ее пределами.

Программное обеспечение (ПО) – совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации данных программ.

Программно-технический комплекс – набор технических и программных средств, работающих совместно в целях выполнения одной или нескольких сходных задач.

Публичная электронная почта – адрес электронной почты, разрешенный для публикации на информационных ресурсах сети «Интернет» и в печатных изданиях.

Сквозная авторизация – автоматическая авторизация пользователя в различных ИС при успешном прохождении аутентификации в службе каталогов.

СКПЭП – сертификат ключа проверки электронной подписи.

Служебная электронная почта – внутренняя или внешняя электронная почта, используемая для переписки в служебных и официальных целях, функционирующая на технических средствах, находящихся в ведении органов (организаций) прокуратуры Российской Федерации.

Служебный персональный компьютер (ПК) – компьютер (АРМ, портативный компьютер), предоставленный органом (организацией) прокуратуры Российской Федерации работнику прокуратуры для выполнения им своих служебных обязанностей при работе в ЗС и ОС ЕЗСПД.

Служба каталога – централизованное средство для именования, хранения и выборки информации, доступное для пользователей, приложений и ИС (например, Active Directory в ЗС и ОС ЕЗСПД).

Служба технической поддержки – представители юридического лица, осуществляющие техническую поддержку средств вычислительной техники и ИС на основании государственного контракта.

Служебная информация – информация, полученная или созданная работниками органов (организаций) прокуратуры при осуществлении своих служебных обязанностей.

Средства вычислительной техники (СВТ) – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем (ПК, АРМ, портативный компьютер и т. д.).

Средства электронной подписи – шифровальные (криптографические) средства, используемые для реализации хотя бы одной из следующих функций: создание электронной подписи, проверка электронной подписи, создание ключа электронной подписи и ключа проверки электронной подписи.

Технические средства – совокупность систем, машин, приборов, механизмов, устройств и прочих видов оборудования, предназначенных для автоматизации технологических процессов информатики, выходным продуктом которых является информация (данные).

Токен – компактное аппаратное устройство, предназначенное для обеспечения идентификации его владельца в информационной системе, безопасного удаленного доступа к информационным ресурсам, а также хранения ключа электронной подписи.

Угроза информационной безопасности органов прокуратуры Российской Федерации – совокупность условий и факторов, создающих опасность нарушения защищенности информации, принадлежащей органам прокуратуры Российской Федерации, и поддерживающей ее информационной инфраструктуры.

Уполномоченное подразделение (работник) – подразделение (должностное лицо), на которое в соответствии с организационно-распорядительным документом органа (организации) прокуратуры Российской Федерации возложены определенные обязанности по организации работы в ИС, на СВТ или их обслуживанию, а также по обеспечению информационной безопасности.

Учетная запись – совокупность данных (логин и пароль), позволяющих получить доступ к информационному ресурсу, информационной системе или СВТ.

Учетные данные – дополнительная информация для учетной записи (ФИО, подразделение, отпечаток СКЭП и т. д.).

Учтенный машинный носитель информации – учтенный в установленном порядке МНИ, позволяющий однозначно определить его владельца.

Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и используется для определения лица, подписывающего информацию.

RSNET – российский государственный сегмент сети «Интернет», который используется для подключения к сети «Интернет» государственных информационных систем и информационно-телекоммуникационных сетей государственных органов, а также для публикации в сети «Интернет» информации государственных органов (организаций).

3. Стандартизация СВТ и программного обеспечения ИСОП

3.1. На всех служебных персональных и портативных компьютерах, а также серверах, подключенных к ИСОП, используется лицензионное либо свободно распространяемое ПО, включая операционные системы (далее – ОС) семейства Windows, либо свободно распространяемые ОС, обеспечивающие функционирование актуальных средств защиты информации, средств электронной подписи и необходимого прикладного ПО.

Список ПО, используемого в органах (организациях) прокуратуры Российской Федерации, утверждается распоряжением заместителя Генерального

прокурора Российской Федерации, курирующего деятельность Главного управления правовой статистики и информационных технологий.

3.2. Решение об установке ПО, необходимого пользователю для выполнения его служебных обязанностей, принимает уполномоченное подразделение или служба технической поддержки.

Установка, переустановка, изменение аппаратной конфигурации служебного ПК, локальной вычислительной сети, ключевых параметров ОС и прикладного ПО, параметров, затрагивающих вопросы информационной безопасности, пользователю запрещены.

3.3. Средства вычислительной техники, подключаемые к ИСОП, должны находиться на балансе (в том числе на забалансовых счетах) органа прокуратуры Российской Федерации. Подключение личных СВТ к ИСОП не допускается.

Аппаратная конфигурация СВТ должна соответствовать техническим требованиям, необходимым для функционирования используемых в ИСОП версий ОС, средств защиты информации, средств электронной подписи и прикладного ПО.

3.4. Техническое обслуживание СВТ, настройку, подключение к локальной вычислительной сети обеспечивает уполномоченное подразделение или служба технической поддержки.

3.5. Размещение ИС и ИР органов прокуратуры Российской Федерации допускается исключительно в ЗС или ОС ЕЗСПД, если организационно-распорядительными документами Генеральной прокуратуры Российской Федерации не установлен иной порядок.

3.6. Использование на СВТ в ИСОП устройств для организации беспроводных каналов связи запрещено, за исключением централизованно поставляемого Генеральной прокуратурой Российской Федерации оборудования, реализующего удаленный доступ с соблюдением требований информационной безопасности. Не допускается использование беспроводных кликеров, компьютерных мышек, клавиатур.

3.7. Обладателем всей информации, хранимой и обрабатываемой на служебных ПК, является соответствующий орган прокуратуры Российской Федерации.

4. Порядок регистрации пользователей средств вычислительной техники, наделение их полномочиями доступа к информационным системам и информационным ресурсам

4.1. С целью соблюдения персональной ответственности за свои действия для каждого пользователя СВТ органов прокуратуры Российской Федерации создается уникальная учетная запись, под которой он регистрируется в службе каталогов ИСОП как для работы на служебном ПК, так и для работы в ИС.

Если для доступа к служебному ПК или ИС нет возможности использовать учетную запись службы каталогов ИСОП (сквозную авторизацию), пользователю

создается учетная запись, схожая по написанию с учетной записью, под которой он зарегистрирован в службе каталогов ИСОП, или учетная запись, содержащая учетные данные, однозначно идентифицирующие данного пользователя.

Использование несколькими работниками одного и того же имени пользователя (группового имени) при работе в ИСОП запрещается.

4.2. Процедуры регистрации пользователя СВТ и предоставления (изменения, блокировки) ему прав доступа к ИС или ИР ИСОП осуществляются уполномоченным подразделением или службой технической поддержки на основании заявки (приложение № 1), если организационно-распорядительными документами Генеральной прокуратуры Российской Федерации не установлен иной порядок.

4.3. Заявка направляется посредством АИК «Надзор-WEB» в адрес уполномоченного подразделения Генеральной прокуратуры Российской Федерации за подписью заместителя руководителя органа прокуратуры Российской Федерации, в адрес уполномоченного подразделения прокуратуры субъекта Российской Федерации, приравненной к ней специализированной прокуратуры, прокуратуры комплекса «Байконур» (далее – прокуратура субъекта Российской Федерации) – за подписью руководителя подразделения органа прокуратуры Российской Федерации, в котором работает пользователь.

Заявки в адрес службы технической поддержки направляются посредством внутренней электронной почты ИСОП или соответствующего сервиса подачи электронных заявок.

4.4. В заявке указываются:

должность (с полным наименованием подразделения);

ФИО работника;

контактные данные работника (адрес электронной почты, номер телефона);

задачи, для выполнения которых работнику требуется запрашиваемый доступ (при необходимости);

наименование СВТ или ИС, к которым необходимо получить доступ;

содержание запрашиваемых действий (регистрация нового пользователя, изменение прав доступа к ИС или ИР ранее зарегистрированного пользователя).

4.5. В исключительных случаях по распоряжению руководителя органа прокуратуры Российской Федерации допускается самостоятельное создание учетных записей уполномоченным подразделением органа прокуратуры Российской Федерации согласно штатному расписанию. При этом создание, изменение регистрационных данных и персональных прав доступа осуществляются на основании кадровых приказов в соответствии со служебными обязанностями данного работника.

4.6. Основаниями для блокировки (удаления) учетной записи пользователя СВТ (в том числе доступ в сеть «Интернет»), изменения прав доступа или прекращения доступа к ИС или ИР являются увольнение, перевод в другой орган или подразделение прокуратуры, изменение служебных обязанностей пользователя, отсутствие более 6 месяцев по причине командировки или болезни.

Блокировка осуществляется уполномоченным подразделением (работником) по мотивированной заявке.

4.7. Уполномоченное подразделение или служба технической поддержки рассматривает представленную заявку в установленные сроки и сообщает о результатах ее исполнения заявителю.

Если организационно-распорядительными документами Генеральной прокуратуры Российской Федерации, прокуратуры субъекта Российской Федерации не установлено иное, срок рассмотрения заявки составляет:

для Генеральной прокуратуры Российской Федерации – до 30 рабочих дней;

для прокуратуры субъекта Российской Федерации – до 3 рабочих дней;

для службы технической поддержки срок устанавливается государственным контрактом.

4.8. Работнику, зарегистрированному в качестве нового пользователя СВТ или ИС, сообщается соответствующее ему имя пользователя, выдается начальное значение пароля, которое он обязан при наличии такой возможности сменить при первой авторизации.

5. Правила организации парольной защиты, порядок передачи и хранения паролей

5.1. В целях обеспечения защиты от несанкционированного доступа при использовании учетных записей в ИСОП и подтверждения идентификации пользователя служебного ПК или ИС применяются пароли.

5.2. Первоначальное создание паролей осуществляется уполномоченным подразделением или службой технической поддержки.

5.3. Сменяемые личные пароли выбираются пользователем самостоятельно с учетом следующих требований:

длина пароля должна быть не менее 8 символов;

среди символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы;

пароль не должен включать в себя легко вычисляемые сочетания символов (простая последовательность цифр или букв, имена, фамилии, наименования рабочих станций и т. д.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях.

5.4. Периодичность смены пароля пользователя устанавливается в соответствии с настройками безопасности конкретных СВТ или ИС.

Допускается использование постоянного пароля пользователя, если организационно-распорядительными документами Генеральной прокуратуры Российской Федерации или техническими требованиями в отношении конкретных СВТ или ИС не установлен иной порядок.

5.5. В случае компрометации (утери, передачи другому лицу) личного пароля пользователь должен принять незамедлительные меры для смены пароля,

а также сообщить об этом в уполномоченное подразделение или службу технической поддержки.

Внеплановая смена (блокировка) пароля в случаях его компрометации производится на основании заявки в порядке пункта 4.2 настоящей Инструкции уполномоченным подразделением или службой технической поддержки, в том числе на основании копии приказов о приеме (увольнении, переводе) работников органов прокуратуры.

5.6. Хранение значений действующих паролей в электронном виде допускается на СВТ или ИС, обеспечивающих авторизованный доступ исключительно владельцу пароля.

Хранение значений действующих паролей на бумажном носителе или съемных МНИ допускается только в прочных надежно запираемых хранилищах (сейфах, ящиках), исключающих доступ посторонних лиц.

5.7. Передача паролей пользователям осуществляется уполномоченным подразделением или службой технической поддержки. Передача личных паролей пользователем запрещена.

Если организационно-распорядительными документами Генеральной прокуратуры Российской Федерации не установлен иной порядок, передача паролей осуществляется следующими способами:

направляется на бумажных носителях или съемных МНИ с присвоением грифа «Для служебного доступа»;

сообщается лично пользователю, в том числе посредством сервиса единой системы ведомственной телефонной связи (ЕСВТС) или прямого сеанса ВКС;

высылается пользователю на именную почту ИСОП (только временные пароли, требующие смены).

Передавать в электронном виде открытое значение пароля совместно с именем (логином) учетной записи по любым каналам связи, в том числе посредством АИК «Надзор-WEB», запрещается.

6. Порядок организации антивирусной защиты

6.1. К использованию на СВТ и в ИС органов прокуратуры Российской Федерации допускаются только лицензионные средства антивирусной защиты, централизованно закупленные и рекомендуемые к применению уполномоченным подразделением Генеральной прокуратуры Российской Федерации.

6.2. Установка и настройка средств антивирусной защиты на СВТ осуществляется уполномоченным подразделением или службой технической поддержки.

Самостоятельная установка или изменение параметров средств антивирусной защиты пользователем СВТ запрещена.

6.3. Используемые на СВТ средства антивирусной защиты должны иметь индикаторы работоспособности и текущего статуса. При обнаружении отсутствия индикации или в случае, если индикация указывает на

неработоспособность средства антивирусной защиты, пользователь обязан уведомить о данном факте уполномоченное подразделение прокуратуры или службу технической поддержки.

6.4. В начале работы при включении СВТ, а также при первом доступе к файлам в автоматическом режиме проводится их антивирусный контроль.

6.5. Обязательному антивирусному контролю подлежит любая внешняя информация (файлы документов любых форматов, файлы данных, исполняемые файлы), получаемая и передаваемая по телекоммуникационным каналам посредством сети «Интернет», а также информация, полученная посредством съемных МНИ.

6.6. Контроль внешней входящей информации в случае ее получения по телекоммуникационным каналам необходимо проводить непосредственно после ее приема, а информации, получаемой посредством съемных МНИ, – до ее приема. Контроль производится на СВТ, имеющих средства антивирусной защиты, находящиеся в актуализированном и работоспособном состоянии. В случае отсутствия такой возможности необходимо обратиться в уполномоченное подразделение или службу технической поддержки.

6.7. При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, замедление работы, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т. п.) пользователь СВТ должен незамедлительно уведомить о данном факте уполномоченное подразделение или службу технической поддержки, а также по возможности провести самостоятельно внеочередной антивирусный контроль СВТ для определения факта наличия или отсутствия компьютерного вируса.

6.8. В случае обнаружения при проведении антивирусного контроля фактов зараженных компьютерными вирусами файлов пользователь СВТ обязан:

приостановить работу на СВТ;

незамедлительно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя своего подразделения, владельца зараженных файлов, смежные подразделения, использующие эти файлы в работе, а также проинформировать уполномоченное подразделение или службу технической поддержки.

6.9. Периодический контроль состояния антивирусной защиты на СВТ, соблюдения установленного порядка антивирусного контроля и выполнения требований настоящей Инструкции осуществляется уполномоченным подразделением соответствующего органа прокуратуры Российской Федерации, ответственным за обеспечение информационной безопасности.

6.10. Работники органов прокуратуры Российской Федерации обязаны не реже одного раза в месяц самостоятельно осуществлять полную антивирусную проверку своих служебных СВТ. Контроль за выполнением данных требований возлагается на руководителей подразделений органов прокуратуры Российской Федерации.

6.11. Работники органов прокуратуры Российской Федерации по мере

необходимости производят резервное копирование своих критически важных служебных документов на внешние МНИ.

7. Порядок организации работы со средствами электронной подписи

7.1. Пользователь органов прокуратуры Российской Федерации использует средства электронной подписи при осуществлении своей профессиональной служебной деятельности в объеме, определенном служебными обязанностями.

7.2. Основанием для оформления СКПЭП является назначение пользователя на должность или возложение на пользователя функциональных обязанностей, требующих использования средств электронной подписи.

7.3. Для оформления СКПЭП пользователь формирует пакет документов и выполняет действия согласно организационно-распорядительным документам аккредитованного удостоверяющего центра, в котором происходит создание СКПЭП.

7.4. Пользователю надлежит своевременно производить плановую смену СКПЭП в установленные сроки и способом, предусмотренным организационно-распорядительными документами аккредитованного удостоверяющего центра.

7.5. При использовании средств электронной подписи пользователь обязан выполнять и другие требования, установленные нормативными правовыми актами Российской Федерации, регулирующими использование средств электронной подписи, документами аккредитованного удостоверяющего центра, в котором изготовлен используемый СКПЭП, организационно-распорядительными документами Генеральной прокуратуры Российской Федерации, а также органа прокуратуры Российской Федерации, в котором он осуществляет свою профессиональную служебную деятельность.

8. Порядок организации работы с электронной почтой

8.1. Для исполнения своих служебных обязанностей и обмена информацией в электронном виде сотрудникам органов прокуратуры Российской Федерации предоставляется персональная внутренняя почта ИСОП.

При необходимости сотруднику может быть предоставлена внешняя почта ИСОП, зарегистрированная как на должностное лицо, так и на подразделение органа прокуратуры Российской Федерации.

8.2. Электронная почта предназначена для обмена служебной информацией в электронном виде. Передача информации ограниченного распространения посредством электронной почты не допускается.

8.3. Сервисы электронной почты органов прокуратуры Российской Федерации как внутренней, так и внешней, а также хранимая на них информация, располагаются в сети ИСОП.

8.4. Поручения, сообщения, указания, пересылаемые по электронной почте, предназначены для оперативной доставки информации и носят информационно-

уведомительный характер как дополнение к документам, направляемым на бумажных носителях или посредством АИК «Надзор-WEB».

8.5. Отправка служебных документов, содержащих резолюции, подписи, печати, штампы и так далее, разрешается только с использованием почтовых сервисов органов прокуратуры Российской Федерации. Данные документы должны иметь формат электронного документа или быть отсканированы и сохранены в графический формат PDF с разрешением не менее 300 dpi.

8.6. Проверка почтового ящика (получение почты) осуществляется сотрудниками не реже четырех раз в течение рабочего дня.

8.7. При использовании внешней электронной почты ИСОП отправитель в обязательном порядке в тексте письма указывает свои ФИО, должность и номер контактного телефона.

8.8. Ответственность за передаваемую посредством электронной почты информацию несет ее отправитель.

8.9. Информация, поступившая на официальные адреса электронной почты органа прокуратуры Российской Федерации, должна быть при необходимости зарегистрирована в АИК «Надзор-WEB» и незамедлительно передана работнику, которому она адресована.

8.10. Создание (удаление) внутреннего электронного почтового ящика ИСОП осуществляется службой технической поддержки органов прокуратуры Российской Федерации или автоматически при регистрации пользователя в ИСОП.

8.11. Создание (удаление) электронного почтового ящика внешней почты ИСОП осуществляется уполномоченным подразделением на основании заявки (приложение № 2).

Заявка направляется посредством АИК «Надзор-WEB» в адрес уполномоченного подразделения Генеральной прокуратуры Российской Федерации за подписью руководителя структурного подразделения Генеральной прокуратуры Российской Федерации, в адрес уполномоченного подразделения прокуратуры субъекта Российской Федерации – за подписью руководителя подразделения органа прокуратуры Российской Федерации, в котором работает пользователь.

8.12. В заявке указываются:

должность (с полным наименованием подразделения);

ФИО работника;

контактные данные работника (адрес внутренней электронной почты ИСОП, номер телефона);

задачи, для выполнения которых работнику требуется электронная почта (при необходимости);

формат электронной почты (на подразделение или персональная).

8.13. При формировании имени электронной почты используется ГОСТ 7.79-2000 (ИСО 9-95) «Правила транслитерации кириллического письма латинским алфавитом» (Система Б), утвержденный для перевода кириллических

символов в символы латинского алфавита.

8.14. Пользователь СВТ должен регулярно очищать свою электронную почту. Не рекомендуется отправлять электронные письма размером больше, чем 15 Мбайт при использовании внутренней почты ИСОП и 20 Мбайт при использовании внешней почты ИСОП. Для уменьшения размера электронного письма передаваемые файлы могут быть упакованы стандартной программой сжатия (архиватором) ZIP.

9. Порядок организации работы с видео-конференц-связью

9.1. Для надлежащей организации и сопровождения проведения мероприятий в режиме ВКС в органах прокуратуры Российской Федерации необходимо направлять заявку на организацию и сопровождение проведения мероприятий в режиме ВКС (приложение № 3) не менее чем за 2 рабочих дня до даты его проведения. В Генеральной прокуратуре Российской Федерации заявка направляется в Главное управление правовой статистики и информационных технологий, в прокуратуре субъекта Российской Федерации – в подразделение прокуратуры субъекта Российской Федерации, ответственное за техническое сопровождение мероприятий в режиме ВКС.

9.2. В заявке указывается следующая информация:

запланированные дата и время проведения мероприятия в режиме ВКС;

запланированные дата и время проведения тестовых сеансов связи в режиме ВКС (при отсутствии указанной информации в заявке дата и время тестовых подключений могут назначаться подразделением органа прокуратуры, ответственным за техническое сопровождение мероприятий в режиме ВКС);

контактные телефоны ответственных за организацию проведения ВКС (подразделение органа прокуратуры – инициатор проведения ВКС);

контактные телефоны ответственных за техническое сопровождение мероприятий в режиме ВКС со стороны организаторов, если ВКС проводится в ОС ЕЗСПД сторонней организацией;

полные ФИО участников ВКС с указанием подразделения;

контактные телефоны (внутренние, городские, при необходимости мобильные) участников ВКС;

номера кабинетов и зданий (для работников Генеральной прокуратуры Российской Федерации);

дополнительная информация о подключении, предоставленная организатором мероприятия в режиме ВКС (при наличии);

номер виртуальной комнаты Avaya (если ВКС проводится в ЗС ЕЗСПД), предварительно согласованный с подразделением органа прокуратуры Российской Федерации, ответственным за техническое сопровождение мероприятий в режиме ВКС;

необходимость ведения видеозаписи мероприятия в режиме ВКС;

потребность в трансляции демонстрационных материалов, показ работы ПО.

9.3. После согласования даты и времени проведения ВКС подразделением, ответственным за организацию ВКС (инициатор ВКС), издается регламент проведения ВКС (приложение № 4), который направляется всем участникам ВКС посредством АИК «Надзор-WEB». При необходимости уведомления о проведении ВКС могут направляться участникам ВКС через внутреннюю или внешнюю почту ИСОП.

9.4. Подразделение, ответственное за техническое сопровождение ВКС, обеспечивает:

работоспособность оборудования ВКС;

инструктаж участников ВКС;

техническую помощь участникам ВКС;

при необходимости включение, отключение, регулировку уровня микрофонов, видеокамер, динамиков участников ВКС;

техническую организацию трансляции демонстрационных материалов участникам ВКС;

техническую организацию видеозаписи ВКС;

расположение, переключение, отключение раскладки экранов участников ВКС.

9.5. Подразделение, ответственное за организацию ВКС (инициатор ВКС), обеспечивает:

издание регламента проведения ВКС и доведение его до всех участников ВКС;

организацию сбора всех участников ВКС для проведения ВКС или предварительного теста ВКС;

своевременное предоставление демонстрационных материалов подразделению органа прокуратуры Российской Федерации, ответственному за техническое сопровождение ВКС.

9.6. Участники ВКС обеспечивают:

включение и отключение микрофонов в ходе выступления;

уровень освещенности, позволяющий четко видеть участника ВКС;

отключение всех посторонних источников звука (работающие приборы, открытые окна, двери и так далее) в помещении, где проводится ВКС;

отсутствие посторонних лиц рядом с участником ВКС, попадающих в поле зрения видеокамеры.

9.7. Общие требования к проведению мероприятий в режиме ВКС с участием руководителей Генеральной прокуратуры Российской Федерации и прокуратур субъектов Российской Федерации.

В кадре должны отображаться:

по центру – выступающий (крупным планом, сидящий за столом или стоящий за трибуной, при этом руки не должны обрезаться краем кадра);

по центру над выступающим – герб Российской Федерации

(при наличии не должен обрезаться краями кадра);

справа от выступающего – флаг Российской Федерации;

слева от выступающего – флаг прокуратуры Российской Федерации.

Микрофоны необходимо включать только после предоставления выступающему (спикеру) слова. Во избежание появления посторонних звуков во время проведения ВКС у остальных участников ВКС микрофоны должны быть выключены.

9.8. Во избежание случаев проведения одновременно нескольких мероприятий в режиме ВКС подразделением, ответственным за техническое сопровождение ВКС, составляется и ведется график проведения мероприятий в режиме ВКС. Указанный график, инструкция по работе с ПО Avaya, видеозаписи (при необходимости и допустимости) проведенных мероприятий в режиме ВКС и другие материалы должны размещаться на общедоступном ресурсе в закрытом сегменте ЕЗСПД:

для ВКС, проводимых Генеральной прокуратурой Российской Федерации, по адресу: \\fsgpgvc02\Информационно-аналитические материалы\34. ВКС ГПРФ;

для ВКС, проводимых в прокуратурах субъектов Российской Федерации и приравненных к ним специализированных прокуратурах, на самостоятельно определенном общедоступном ресурсе.

10. Порядок оказания технической поддержки. Обслуживание средств вычислительной, организационной техники (обновление, ремонт, передача, списание) и программного обеспечения

10.1. Техническая поддержка и сопровождение программно-технических комплексов и ИС, разработанных или внедренных по заданию Генеральной прокуратуры Российской Федерации, осуществляются разработчиком (поставщиком) соответствующего программно-технического комплекса, ИС или специализированной организацией в рамках исполнения обязательств по заключенному государственному контракту.

10.2. Контактные данные и порядок обращения в службу технической поддержки программно-технического комплекса, ИС публикуются на первой странице интерфейса пользователя, в эксплуатационной документации, в соответствующем государственном контракте, в иных официальных документах Генеральной прокуратуры Российской Федерации.

Перечень используемых программно-технических комплексов и ИС, телефоны служб технической поддержки, подразделений, отвечающих за техническое или методическое сопровождение данных систем, должны размещаться на общедоступном ресурсе в закрытом сегменте ЕЗСПД:

в Генеральной прокуратуре Российской Федерации – по адресу: \\fsgpgvc02\Информационно-аналитические материалы\35. ТехПод ГПРФ, а также на Едином портале прокуратуры Российской Федерации;

в прокуратурах субъектов Российской Федерации – на самостоятельно

определенном общедоступном ресурсе.

10.3. При возникновении неисправностей, препятствующих надлежащей работе программно-технического комплекса, ИС, пользователь самостоятельно обращается в службу технической поддержки, если иное не указано в организационно-распорядительных документах Генеральной прокуратуры Российской Федерации, устанавливающих правила эксплуатации соответствующего комплекса или системы.

10.4. При обращении в службу технической поддержки пользователь должен кратко описать возникшую неисправность, при необходимости уточнить, какие действия следует предпринять. Для связи со специалистами службы технической поддержки в обязательном порядке сообщить контактный номер телефона.

10.5. При направлении в службу технической поддержки фото- и видеоматериалов, иллюстрирующих неисправность, запрещается передача персональных данных, иной конфиденциальной информации, которые могут содержаться на копии или фотографии экрана, а также попасть в кадр на заднем плане.

10.6. В целях исключения подачи в службу технической поддержки необоснованных заявок, не связанных с неисправностями, препятствующих корректной работе, пользователь обязан изучать актуальные инструкции по эксплуатации программно-технического комплекса, ИС.

10.7. В случае возникновения критической неисправности программно-технического комплекса, ИС, повлекшей простой в работе с нарушением сроков исполнения поручений, заданий, пользователь обязан доложить об этом обстоятельстве непосредственному начальнику.

Справки об имевшей место критической неисправности программно-технического комплекса, ИС оформляются уполномоченным подразделением (работником) по запросам руководителей органов прокуратуры Российской Федерации, начальников структурных подразделений.

10.8. Пользователь несет полную ответственность за сохранность и надлежащую эксплуатацию переданных ему с оформлением соответствующих документов (опись закрепленных за пользователем материальных средств) СВТ как принадлежащих органам прокуратуры Российской Федерации, так и предоставленных в пользование по сервисной модели в соответствии с условиями государственного контракта.

10.9. Пользователь обязан по требованию материально ответственного лица или членов комиссии, проводящей инвентаризацию в органе прокуратуры Российской Федерации, предъявить переданные ему СВТ в исправном состоянии.

В случае отсутствия материальных средств или их ненадлежащего состояния (неисправность, некомплектность) пользователь представляет письменные объяснения с приложением подтверждающих документов. Решение об инициировании проверки обстоятельств повреждения или утраты пользователем материальных средств принимается в соответствии с

действующими организационно-распорядительными документами Генеральной прокуратуры Российской Федерации, прокуратуры субъекта Российской Федерации.

10.10. Пользователям запрещается самостоятельно перемещать между рабочими кабинетами СВТ. В случае служебной необходимости перемещение производится только с согласия материально ответственного лица после информирования уполномоченного подразделения (работника) для внесения изменений в схемы подключения и учетные записи.

10.11. Выданные по сервисной модели СВТ при переводе пользователя из одного подразделения в другое в Генеральной прокуратуре Российской Федерации или прокуратуре субъекта Российской Федерации остаются закрепленными за данным пользователем. Перемещение производится на основании заявки в техническую поддержку организации, которой в рамках государственного контракта осуществлено предоставление указанного комплекта техники.

10.12. До передачи СВТ от одного пользователя другому без изменения места размещения СВТ пользователем в обязательном порядке ставится в известность материально ответственное лицо, а также самостоятельно или при необходимости с привлечением работников уполномоченного подразделения производятся очистка СВТ от служебной информации (документов) и подготовка СВТ к выдаче новому пользователю.

В случае необходимости передачи своей служебной информации (документов) новому пользователю СВТ данная информация размещается в папке с ФИО предыдущего пользователя СВТ.

10.13. При увольнении работника СВТ подлежат возврату в уполномоченное подразделение для подготовки к выдаче иному пользователю, о чем одновременно ставится в известность материально ответственное лицо, если иные условия не предусмотрены государственным контрактом по предоставлению в пользование СВТ по сервисной модели.

10.14. Пользователь обязан незамедлительно поставить в известность непосредственного руководителя о выходе из строя, повреждении, утрате вверенных ему СВТ.

Руководитель структурного подразделения Генеральной прокуратуры Российской Федерации и органа прокуратуры Российской Федерации направляет информацию о выходе из строя, повреждении, утрате СВТ материально ответственному лицу и уполномоченному подразделению для принятия мер по ремонту или замене технических средств, а также принимает решение об инициировании проверки обстоятельств повреждения или утраты материальных средств.

10.15. Ремонт СВТ производится в организации, осуществляющей гарантийный ремонт или ремонт за счет средств федерального бюджета, с которой органом прокуратуры Российской Федерации заключен государственный контракт. Ремонт в иных организациях должен быть согласован с

уполномоченным подразделением.

10.16. До передачи СВТ сторонним организациям в ремонт производится при наличии технической возможности демонтаж МНИ либо полная очистка данных с МНИ без возможности восстановления.

На подлежащих списанию СВТ производится полная очистка данных с МНИ без возможности восстановления либо физическое уничтожение таких МНИ. В случае целесообразности и возможности повторного использования МНИ демонтируют с СВТ. О произведенных действиях составляется акт. Мероприятия по списанию и утилизации СВТ осуществляются работниками уполномоченных подразделений.

10.17. Плановое техническое обслуживание и обновление ПО СВТ производятся работниками уполномоченного подразделения или службой технической поддержки по согласованию с пользователем. Внеплановое техническое обслуживание производится незамедлительно в случаях:

обнаружения вирусной активности;

подозрения на постороннее вмешательство в работу СВТ;

предотвращения утечки информации или другого нарушения информационной безопасности;

выявления неисправности, угрожающей потерей критически важных данных, нарушением работоспособности отдельных СВТ или ИСОП в целом.

10.18. Пользователь, прошедший соответствующий инструктаж в уполномоченном подразделении, самостоятельно производит замену расходных материалов в переданной ему копировально-множительной и печатающей оргтехнике, если иное не предусмотрено условиями государственного контракта или организационно-распорядительными документами Генеральной прокуратуры Российской Федерации, устанавливающими правила эксплуатации соответствующего программно-технического комплекса.

10.19. Выдача и учет расходных материалов (офисная бумага, картриджи, тонеры и так далее) для копировально-множительной и печатающей оргтехники в органах прокуратуры Российской Федерации осуществляются подразделением, ответственным за материально-техническое обеспечение.

Не допускается возложение обязанностей по выдаче и учету расходных материалов для копировально-множительной и печатающей оргтехники на подразделения, осуществляющие сопровождение ИС в органах прокуратуры Российской Федерации.

Не допускается возложение полной материальной ответственности за СВТ и оргтехнику на подразделения, осуществляющие сопровождение информационных систем в органах прокуратуры Российской Федерации.

11. Порядок предоставления доступа и осуществления работы в сети «Интернет»

11.1. Основными целями использования в органах прокуратуры Российской

Федерации сети «Интернет» являются:

оперативное получение необходимой информации в служебных целях;

доступ к ИС и работа в ИС, необходимых для исполнения своих служебных обязанностей;

осуществление переписки с использованием служебной электронной почты при исполнении своих служебных обязанностей;

взаимодействие работников органов прокуратуры Российской Федерации с гражданами, представителями иных органов и организаций, включая международные органы и организации, компетентных органов иностранных государств, средств массовой информации и общественности, в том числе в режиме видео-конференц-связи (без направления документов, содержащих информацию ограниченного распространения, сведений конфиденциального характера, а также персональных данных, за исключением общедоступных, на Едином портале прокуратуры Российской Федерации);

информирование граждан о работе органов прокуратуры Российской Федерации, в том числе в рамках официальных ИР органов прокуратуры Российской Федерации;

направление официальных ответов посредством служебной электронной почты на обращения граждан и организаций;

осуществление правового просвещения и правового информирования в порядке, установленном организационно-распорядительными документами Генеральной прокуратуры Российской Федерации;

рассмотрение уведомлений о распространяемой с нарушением закона информации в информационно-телекоммуникационных сетях, в том числе в сети «Интернет».

11.2. Подключение органов прокуратуры Российской Федерации к сети «Интернет» осуществляется через государственный домен сети RSNet, созданный для федеральных органов государственной власти и находящийся в ведении Федеральной службы охраны Российской Федерации.

11.3. Доступ к ресурсам сети «Интернет» в органах прокуратуры Российской Федерации организуется с использованием «АРМ – Интернет».

11.4. Для защиты от вредоносного программного обеспечения при работе в сети «Интернет» используются лицензионные средства антивирусной защиты с актуальными базами антивирусных сигнатур.

11.5. Процедура предоставления или блокировки пользователю доступа к сети «Интернет» осуществляется на основании заявки (приложение № 1) и в порядке, предусмотренном пунктом 4 настоящей Инструкции, при этом в поле заявки «наименование системы» указывается «сеть «Интернет».

11.6. О причинах временной блокировки, а также необходимых действиях пользователя «АРМ – Интернет» или ответственных лиц ответственный работник (ответственное подразделение), инициировавший блокировку, в кратчайшие сроки извещает пользователя «АРМ – Интернет», либо его

руководителя, либо руководителя органа прокуратуры Российской Федерации.

12. Обязанности и права пользователя

12.1. Пользователь СВТ обязан:

ознакомиться с настоящей Инструкцией и неукоснительно соблюдать ее требования;

производить обмен служебной информацией между органами прокуратуры Российской Федерации и хранение служебной информацией исключительно в ЗС ЕЗСПД, если организационно-распорядительными документами Генеральной прокуратуры Российской Федерации не установлен иной порядок. Обеспечивающими подразделениями (материально-технические, программно-технологические, информационно-технологические, финансово-хозяйственные) допускаются хранение служебной информации и обмен ею в ОС ЕЗСПД в рамках исполнения своих служебных обязанностей;

пользоваться ПО, установленным уполномоченным подразделением или службой технической поддержки;

использовать для переноса информации съемные МНИ, не предназначенные для хранения и обработки сведений, составляющих государственную и иную охраняемую законом тайну;

пользоваться данными своей учетной записи для входа в служебный ПК и для доступа к ИС, ИР ИСОП и сети «Интернет»;

исключить возможность неконтролируемого доступа других лиц к служебному ПК, на котором произведена авторизация пользователя;

хранить свои идентификационные данные и ключевые носители (имена учетных записей, пароли, токены) в местах, исключающих доступ к ним и ознакомление с ними других лиц;

использовать СВТ, ведомственные и иные ИС при работе в ИСОП исключительно для служебной деятельности, предусмотренной должностными инструкциями;

строго соблюдать правила работы на СВТ в соответствии с инструкцией по эксплуатации и настоящей Инструкцией;

завершать корректно используемые программы по окончании работы до выключения питания служебного ПК. Пользователю разрешается не выключать питание служебного ПК после окончания рабочего времени только по согласованию с уполномоченным подразделением;

рационально пользоваться ресурсами СВТ, в том числе дисковой памятью ПК и сетевых папок, пропускной способностью локальной вычислительной сети и расходными материалами организационной техники;

не допускать хранения на ПК посторонних программных средств и неслужебной информации;

выполнять требования по обеспечению информационной безопасности, определенные нормативными правовыми актами Российской Федерации,

организационно-распорядительными документами Генеральной прокуратуры Российской Федерации и прокуратуры субъекта Российской Федерации, а также рекомендациями и предписаниями уполномоченного подразделения;

не допускать обработку служебной информации ограниченного распространения в условиях, позволяющих просматривать ее лицам, не имеющим к ней допуска, а также нарушающих требования по эксплуатации СВТ;

предоставлять доступ к СВТ представителям уполномоченных подразделений и службы технической поддержки для проверки исправности и соответствия установленным правилам работы СВТ;

знать способы выявления нештатных ситуаций при использовании ОС и ПО, меры их предотвращения;

немедленно сообщать в уполномоченное подразделение об обнаруженных проблемах в использовании предоставленных ресурсов, в том числе о фактах несанкционированного доступа к оборудованию, информации, ее искажения или уничтожения, об известных каналах утечки информации, способах и средствах обхода или разрушения механизмов защиты информации, о появлении сообщений антивирусного ПО о потенциальной опасности или факте заражения, а также о нарушении требований настоящей Инструкции кем-либо;

сообщать в службу технической поддержки или уполномоченное подразделение о фактах несоответствия информации идентифицирующего пользователя СВТ и ИС;

незамедлительно уведомлять службу технической поддержки, а при ее отсутствии – уполномоченное подразделение о неисправности СВТ, сбое работоспособности и иных фактах нештатной работы ПО.

12.2. Пользователю СВТ запрещается:

создавать и хранить на служебном ПК, не предназначенном для обработки сведений, составляющих государственную тайну, документы с грифом «секретно», «совершенно секретно» и «особой важности»;

записывать и хранить служебную информацию ограниченного распространения на не учтенных в установленном порядке МНИ;

удалять с обрабатываемых или распечатываемых документов грифы конфиденциальности;

использовать для переноса информации съемные МНИ, предназначенные для хранения и обработки служебной информации ограниченного распространения;

передавать посредством сети «Интернет», в том числе посредством мобильных и иных устройств, документы, содержащие служебную информацию, персональные данные и иные сведения конфиденциального характера (за исключением случаев, когда это прямо предусмотрено федеральным законодательством и организационно-распорядительными документами Генеральной прокуратуры Российской Федерации);

хранить и обрабатывать в сети «Интернет» сведения, содержащие служебную информацию ограниченного распространения;

загружать файлы в сеть «Интернет», а также использовать файлы, полученные из сети «Интернет», без предварительной обработки средствами антивирусной защиты, установленными на «АРМ – Интернет»;

переходить на «АРМ – Интернет» по ссылкам в почтовых сообщениях, полученных от неизвестных источников;

использовать на «АРМ – Интернет» в режиме онлайн радио, телевидение, кинотеатры, за исключением случаев, когда этого требует исполнение служебных обязанностей;

загружать на «АРМ – Интернет» любое ПО, аудио- и видеофайлы, не имеющие отношения к исполнению служебных обязанностей;

осуществлять доступ с «АРМ – Интернет» к интернет-ресурсам, содержание и направленность которых запрещены законодательством Российской Федерации, а также не имеющим отношения к исполнению служебных обязанностей (социальные сети, игровые порталы, файловые хранилища и т. п.);

использовать адрес служебной внешней электронной почты ИСОП для оформления подписки на периодическую рассылку материалов из сети «Интернет», не связанных с исполнением служебных обязанностей;

использовать служебную электронную почту в личных целях;

устанавливать, переустанавливать, удалять, изменять настройки основных параметров ОС и прикладного ПО, а также настройки средств защиты информации;

самостоятельно устанавливать или запускать на служебном ПК любое ПО с внешних МНИ или загруженное из сети «Интернет»;

повреждать, уничтожать или изменять без наличия оснований и полномочий информацию, размещенную на общедоступных ИР в ИСОП;

самостоятельно подключать к СВТ и ИС какие-либо устройства, дополнительное оборудование, имеющие и обеспечивающие доступ к сети «Интернет»;

самовольно подключать СВТ к открытому сегменту ЕЗСПД, а также изменять сетевые настройки;

подключать к структурированным кабельным системам органов прокуратуры Российской Федерации не предназначенные для этого технические средства, в том числе любые личные технические средства;

использовать права доступа к СВТ и ИС с ролью администратора;

осуществлять попытки несанкционированного доступа к СВТ и ресурсам ИСОП;

отключать (блокировать) средства защиты информации;

распространять без соответствующего разрешения в сети «Интернет» в любом виде информацию служебного характера, полученную из ИС и ИР ИСОП;

сообщать кому-либо устно или письменно свои учетные данные и передавать идентификаторы для доступа к СВТ и ИС, а также предоставлять доступ посторонним лицам к СВТ и ИС под своей учетной записью;

использовать, распространять и хранить программы, предназначенные для осуществления несанкционированного доступа, взлома паролей, для нарушения функционирования компьютерного оборудования и компьютерных сетей, а также компьютерные вирусы и любые программы, ими зараженные; использовать, распространять и хранить программы сетевого управления и мониторинга, осуществляющие сканирование сети;

хранить на СВТ и ИР ИСОП не относящуюся к выполнению служебных обязанностей работника постороннюю информацию;

совершать действия, способные нанести ущерб информационной безопасности органов прокуратуры Российской Федерации;

производить иные действия, ограничения на которые предусмотрены нормативными правовыми актами Российской Федерации, организационно-распорядительными документами Генеральной прокуратуры Российской Федерации.

12.3. Пользователь СВТ имеет право:

на обеспечение СВТ и ПО, необходимыми ему для исполнения своих служебных обязанностей;

предоставление доступа к ИС и информационным ресурсам, необходимым ему для исполнения своих служебных обязанностей;

обеспечение расходными материалами для компьютерной и организационной техники в количестве, установленном нормами положенности Генеральной прокуратуры Российской Федерации, государственными контрактами;

техническую поддержку при работе на СВТ и в ИС;

обеспечение необходимыми инструкциями, руководствами, документами при работе с СВТ и в ИС при исполнении своих служебных обязанностей;

внесение предложений уполномоченному подразделению по оптимизации настроек служебного ПК, локальной вычислительной сети, ключевых параметров операционной системы и прикладного ПО;

направление заявки в техническую поддержку, а при ее отсутствии – в уполномоченное подразделение на устранение неисправности аппаратной и программной части СВТ;

получение консультации в службе технической поддержки, а при ее отсутствии – в уполномоченном подразделении по работе с СВТ и ПО по вопросам информационной безопасности.

13. Ответственность за нарушение требований настоящей Инструкции

13.1. Ответственность за выполнение требований Инструкции возлагается в Генеральной прокуратуре Российской Федерации на руководителей структурных подразделений, а в прокуратурах субъектов Российской Федерации – на руководителей и их заместителей, курирующих вопросы

информационных технологий.

13.2. Персональную ответственность несут:

начальники структурных подразделений Генеральной прокуратуры Российской Федерации, прокуроры субъектов Российской Федерации – за недоведение (несвоевременное доведение) до сведения подчиненных работников требований настоящей Инструкции;

пользователи СВТ – за несоблюдение требований Инструкции.

Приложение № 1

к Инструкции по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации

УТВЕРЖДАЮ

Должность руководителя структурного подразделения

_____ ФИО

(подпись)

Дата

ЗАЯВКА

на регистрацию пользователя и предоставление (изменение, блокировку) ему прав доступа к информационным системам (ресурсам, сетям)

Сведения о пользователе	
Структурное подразделение	
ФИО (полностью)	
Должность	
Телефон	
Адрес внутренней почты ИСОП	
Адрес внешней почты ИСОП	
Сведения о системе	
Наименование системы	
Дополнительная информация	
Необходимые действия (регистрация, изменение прав и т. д.)	
Выполняемые задачи	
Примечание	

Приложение № 2

к Инструкции по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации

УТВЕРЖДАЮ

Должность руководителя структурного подразделения

_____ ФИО

(подпись)

Дата

ЗАЯВКА
на создание (удаление) внешнего электронного почтового ящика

Сведения о пользователе	
Структурное подразделение	
ФИО (полностью)	
Должность	
Телефон	
Адрес внутренней почты ИСОП	
Адрес внешней почты ИСОП (указывается при удалении)	
Формат электронной почты (указывается при создании)	
Дополнительная информация	
Выполняемые задачи (указывается при создании)	
Примечание	

Приложение № 3

к Инструкции по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации

УТВЕРЖДАЮ

Должность руководителя структурного подразделения

_____ ФИО

(подпись)

Дата

ЗАЯВКА

на организацию и сопровождение проведения мероприятий в режиме ВКС

Сведения о мероприятии	
Дата и время проведения	
Дата и время тестового сеанса	
Адреса проведения (здание, кабинет)	
Ответственные лица	
Контактная информация (тел.)	
Контактные данные ответственных со стороны организатора (если ВКС в ОС ЕЗСПД)	
Номер виртуальной комнаты Avaya (при наличии)	
Информация об участниках (ФИО, структурное подразделение, номер телефона)	
Дополнительная информация	
Необходимость видеозаписи / аудиозаписи	Да / Нет
Трансляция демонстрационных материалов	Да / Нет
Примечание	

Приложение № 4

к Инструкции по эксплуатации средств вычислительной техники, информационных систем и информационных ресурсов органов прокуратуры Российской Федерации

УТВЕРЖДАЮ

Должность руководителя структурного подразделения

_____ ФИО

(подпись)

Дата

Регламент проведения ВКС
Тема ВКС
Дата

Повестка дня

1.
2.
3.

Председатель ВКС:

Участники ВКС:

Порядок проведения

Время	Тема выступления / выступающий