



АДМИНИСТРАЦИЯ ГУБЕРНАТОРА БРЯНСКОЙ ОБЛАСТИ И ПРАВИТЕЛЬСТВА БРЯНСКОЙ ОБЛАСТИ

ПРИКАЗ

от 23 апреля 2019 г. № 182-пр
г. Брянск

Об утверждении регламента использования сменных носителей информации, инструкции по организации парольной защиты в администрации Губернатора Брянской области и Правительства Брянской области

В целях организации работ по обеспечению информационной безопасности в структурных подразделениях администрации Губернатора Брянской области и Правительства Брянской области:

1. Утвердить прилагаемые:
регламент использования сменных носителей информации в администрации Губернатора Брянской области и Правительства Брянской области;
инструкцию по организации парольной защиты в администрации Губернатора Брянской области и Правительства Брянской области.

2. Руководителям структурных подразделений администрации Губернатора Брянской области и Правительства Брянской области обеспечить ознакомление с содержанием данного приказа сотрудников администрации Губернатора Брянской области и Правительства Брянской области.

Обеспечить хранение листов ознакомления в структурных подразделениях, копии направить в отдел информационных систем хозяйственного управления администрации Губернатора Брянской области и Правительства Брянской области.

3. Настоящий приказ вступает в силу с момента его подписания и подлежит опубликованию на «Официальном интернет-портале правовой информации» (pravo.gov.ru).

4. Контроль за исполнением приказа возложить на начальника отдела информационных систем хозяйственного управления администрации Губернатора Брянской области и Правительства Брянской области Мальченко Л.В.

Заместитель Губернатора



Ю.В. Филипенко

Утвержден
приказом администрации Губернатора
Брянской области и Правительства
Брянской области
от 23 апреля 2019 г. № 182-пр

РЕГЛАМЕНТ
об использовании сменных носителей информации
в администрации Губернатора Брянской области
и Правительства Брянской области

1. Общие положения

1.1. Настоящий регламент об использовании сменных носителей информации в администрации Губернатора Брянской области и Правительства Брянской области (далее – регламент) устанавливает порядок использования сменных носителей информации на автоматизированных рабочих местах администрации Губернатора Брянской области и Правительства Брянской области (далее – администрация) для использования в информационных системах.

1.2. Действие настоящего регламента распространяется на государственных гражданских служащих Брянской области, замещающих должности государственной гражданской службы Брянской области в администрации (далее – гражданские служащие), и работников администрации, замещающих должности, не являющиеся должностями государственной гражданской службы Брянской области (далее – работники).

2. Основные термины, сокращения и определения, используемые
в настоящем регламенте

Администратор ИС – гражданский служащий или работник, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения (далее – ПО) и оборудования вычислительной техники;

пользователь – гражданский служащий или работник администрации, использующий мобильные устройства и носители информации для выполнения своих служебных обязанностей;

автоматизированное рабочее место пользователя – персональный компьютер с прикладным ПО для выполнения определенной служебной задачи (далее – АРМ);

информационная безопасность – комплекс организационно-технических мероприятий, обеспечивающих конфиденциальность, целостность и доступность информации (далее – ИБ);

информационная система администрации – система, обеспечивающая хранение, обработку, преобразование и передачу информации администрации с использованием компьютерной и другой техники (далее – ИС);

мобильное устройство – переносное электронно-вычислительное устройство, способное принимать, отображать, хранить, обрабатывать и передавать информацию;

носитель информации – любой материальный объект, используемый для хранения и передачи электронной информации;

ПК – персональный компьютер;

паспорт ПК – документ, содержащий полный перечень оборудования и программного обеспечения АРМ;

ПО вредоносное – ПО или изменения в ПО, приводящие к нарушению конфиденциальности, целостности и доступности критичной информации;

ПО коммерческое – ПО сторонних производителей (правообладателей), которое предоставляется в пользование на возмездной (платной) основе;

реестр – документ «Реестр разрешенного к использованию ПО», который содержит перечень коммерческого ПО, разрешенного к использованию в администрации.

3. Порядок использования сменных носителей информации

3.1. Под использованием сменных носителей информации в ИС администрации понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и носителями информации.

3.2. Чтение информации со сменных носителей допускается после проведения проверки на отсутствие вредоносного ПО установленными средствами антивирусной защиты.

3.3. Запись информации на сменные носители информации разрешается только пользователям, имеющим разрешение на предоставление доступа к сменным носителям в режиме записи (далее – разрешение).

3.4. Разрешения на предоставление доступа к сменным носителям в режиме записи осуществляются по заявкам руководителей структурных подразделений администрации, подготовленным по форме согласно приложению к настоящему регламенту.

3.5. Процесс предоставления разрешения состоит из следующих этапов:

3.5.1. Подготовка заявки на предоставление доступа к сменным носителям в режиме записи (далее – заявка) осуществляется руководителем структурного подразделения с указанием структурного подразделения, Ф.И.О. и должности пользователя, обоснования необходимости записи на носитель информации.

3.5.2. Согласование подготовленной заявки руководителем администрации или лицом, его замещающим.

3.5.3. Передача заявки в отдел информационных систем хозяйственного управления администрации для выполнения технических настроек.

3.6. При использовании пользователями сменных носителей информации необходимо:

3.6.1. Соблюдать требования настоящего регламента.

3.6.2. Использовать носители информации исключительно для выполнения служебных обязанностей.

3.6.3. Ставить в известность администраторов ИС о любых фактах нарушения требований настоящего регламента.

3.6.4. Ограничить доступ к сменным носителям информации всеми разумными способами.

3.6.5. Извещать администраторов ИС о фактах утраты (кражи) сменных носителей информации.

3.7. При использовании пользователями сменных носителей информации запрещено:

3.7.1. Использовать носители информации для целей, не связанных со служебной деятельностью.

3.7.2. Оставлять носители информации без присмотра, если не предприняты действия по ограничению доступа.

3.8. Администрация оставляет за собой право блокировать или ограничивать использование сменных носителей информации в ИС администрации.

3.9. Информация об использовании пользователями сменных носителей информации в ИС протоколируется и по запросу может быть предоставлена руководителям структурных подразделений, а также руководителю администрации.

3.10. При возникновении подозрений в отношении гражданского служащего или работника администрации о несанкционированном и/или нецелевом использовании сменных носителей информации инициируется проведение служебной проверки в соответствии с действующим законодательством.

3.11. По факту нарушения положений настоящего регламента составляется заключение, которое передается руководителю администрации.

4. Пользователи, нарушившие требования настоящего регламента, несут ответственность в соответствии с действующим законодательством, включая дисциплинарную ответственность.



Приложение
к регламенту использования сменных
носителей информации в администрации
Губернатора Брянской области и Прави-
тельства Брянской области

ФОРМА
заявки на предоставление доступа к сменным носителям в режиме записи

Заместителю Губернатора
Брянской области

Прошу предоставить _____
(должность, наименование структурного

_____ подразделения, Ф.И.О.)

доступ к сменным носителям в режиме записи бессрочно/разово в связи с

(должность)

(Ф.И.О.)



Утверждена
приказом администрации Губернатора
Брянской области и Правительства
Брянской области
от 23 апреля 2019 г. № 182-пр

ИНСТРУКЦИЯ

по организации парольной защиты в администрации Губернатора Брянской области и Правительства Брянской области

1. Настоящая инструкция по организации парольной защиты в администрации Губернатора Брянской области и Правительства Брянской области (далее – инструкция) регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (удаления учетных записей пользователей) в информационных системах администрации Губернатора Брянской области и Правительства Брянской области.

2. Первоначальные пароли доступа к элементам информационной системы выдаются пользователям уполномоченными сотрудниками отдела информационных систем хозяйственного управления администрации Губернатора Брянской области и Правительства Брянской области. При первоначальном входе в систему происходит запрос нового пароля пользователя, соответствующего правилам формирования паролей.

3. Правила формирования пароля:

пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

пароль должен состоять не менее чем из 6 символов;

в пароле должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от А до Z;

б) строчные буквы английского алфавита от а до z;

в) десятичные цифры (от 0 до 9);

г) символы, не принадлежащие алфавитно-цифровому набору (например, !, \$, #, %);

запрещается использовать в качестве пароля имя входа в систему, простые пароли типа «123», «111», «qwerty» и им подобные, а также имена и даты рождения своей личности и своих родственников, клички домашних животных, номера автомобилей, телефонов и другие пароли, которые можно угадать, основываясь на информации о пользователе;

запрещается использовать в качестве пароля один и тот же повторяющийся символ либо повторяющуюся комбинацию из нескольких символов;

запрещается использовать в качестве пароля комбинацию символов, набираемых в закономерном порядке на клавиатуре (например, 1234567 и т.п.);

запрещается выбирать пароли, которые уже использовались ранее.

4. В информационной системе должна быть осуществлена защита аутентификационной информации в процессе ее ввода от возможного использования лицами, не имеющими на это полномочий. Защита обеспечивается исключением отображения для пользователя действительного значения аутентификационной информации. Вводимые символы пароля могут отображаться условными знаками «*», «•» или иными знаками.

5. Количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя, должно быть не более 5. Разблокирование учетной записи происходит автоматически не ранее чем через 15 минут после последней попытки неудачного ввода логина и пароля.

6. После 10 минут бездействия (неактивности) пользователя должно происходить автоматическое блокирование сеанса доступа. Блокирование сеанса доступа пользователя в информационную систему должно сохраняться до прохождения им повторной идентификации и аутентификации.

7. Порядок смены пароля:

полная плановая смена паролей пользователей в ИС должна проводиться регулярно, не реже одного раза в 3 месяца;

полная внеплановая смена паролей должна производиться в случае компрометации пароля данной информационной системы;

в случае компрометации личного пароля пользователя надлежит немедленно ограничить доступ к информации с данной учетной записи до момента вступления в силу новой учетной записи пользователя или пароля.

8. Правила ввода пароля:

ввод пароля должен осуществляться с учетом регистра, в котором пароль был задан;

во время ввода паролей необходимо исключить произнесение его вслух, возможность его подсматривания посторонними лицами или техническими средствами (видеокамерами и др.).

9. Правила хранения пароля:

запрещается хранение пароля в открытом виде на любых видах носителей информации;

запрещается оставлять записанный пароль в местах, где к нему могут получить доступ неуполномоченные лица;

запрещается сообщать другим пользователям личный пароль, произносить пароль вслух.

10. Лица, использующие парольную защиту, обязаны:
четко знать и строго выполнять требования настоящей инструкции
и других руководящих документов в части обеспечения информационной
безопасности;

своевременно сообщать сотрудникам отдела информационных систем
хозяйственного управления администрации Губернатора Брянской области
и Правительства Брянской области об утере, компрометации, несанкцио-
нированном изменении паролей и несанкционированном изменении сроков
действия паролей.

