АДМИНИСТРАЦИЯ ГУБЕРНАТОРА БРЯНСКОЙ ОБЛАСТИ И ПРАВИТЕЛЬСТВА БРЯНСКОЙ ОБЛАСТИ

ПРИКАЗ

Правовое управление администрации Губернатора Брянской области и Правительства Брянской области
ЗАРЕГИСТРИРОВАНО
«13» мая 2024 г.
Регистрационный номер №10240006001

от 6 мая 2024 г. № 230-пр
г. Брянск

О внесении изменений в приказ администрации Губернатора Брянской области и Правительства Брянской области от 23 апреля 2019 года № 182-пр

В соответствии с федеральными законами от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 27 июля 2006 года № 152-ФЗ «О персональных данных»:

1. Внести в приказ администрации Губернатора Брянской области и Правительства Брянской области от 23 апреля 2019 года № 182-пр «Об утверждении регламента использования сменных носителей информации, инструкции по организации парольной защиты в администрации Губернатора Брянской области и Правительства Брянской области» (в редакции приказа администрации Губернатора Брянской области и Правительства Брянской области от 14 сентября 2021 года № 409-пр) следующие изменения:

1.1. Наименование изложить в редакции:

«Об утверждении регламента об использовании сменных носителей информации в администрации Губернатора Брянской области и Правительства Брянской области, регламента об использовании сменных носителей информации в информационной системе персональных данных администрации Губернатора Брянской области и Правительства Брянской области, Инструкции по организации парольной защиты в администрации Губернатора Брянской области и Правительства Брянской области».

1.2. Пункт 1 изложить в редакции:

«1. Утвердить прилагаемые:

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

регламент об использовании сменных носителей информации в информационной системе персональных данных администрации Губернатора Брянской области и Правительства Брянской области;

Инструкцию по организации парольной защиты в администрации Губернатора Брянской области и Правительства Брянской области.».

1.3. Дополнить регламентом об использовании сменных носителей информации в информационной системе персональных данных администрации Губернатора Брянской области и Правительства Брянской области согласно приложению 1 к настоящему приказу.

2. Внести изменения в регламент использования сменных носителей информации в администрации Губернатора Брянской области и Правительства Брянской области, утвержденный вышеуказанным приказом, изложив его в редакции согласно приложению 2 к настоящему приказу.

3. Внести изменения в инструкцию по организации парольной защиты в администрации Губернатора Брянской области и Правительства Брянской области, утвержденную вышеуказанным приказом, изложив ее в редакции согласно приложению 3 к настоящему приказу.

4. Настоящий приказ вступает в силу со дня его подписания и подлежит официальному опубликованию.

5. Ознакомить с настоящим приказом сотрудников администрации Губернатора Брянской области и Правительства Брянской области в части, их касающейся.

6. Контроль за исполнением приказа возложить на начальника отдела информационных технологий администрации Губернатора Брянской области и Правительства Брянской области Марусова А.С.

Заместитель Губернатора Ю.В. Филипенко

Приложение 1
к приказу администрации Губернатора
Брянской области и Правительства
Брянской области
от 6 мая 2024 г. № 230-пр

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

РЕГЛАМЕНТ
об использовании сменных носителей информации в информационной системе персональных данных администрации Губернатора Брянской области и Правительства Брянской области

1. Общие положения

1.1. Настоящий регламент об использовании сменных носителей информации в информационной системе персональных данных 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 персональных данных.

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

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

Информационная система персональных данных – система, обеспечивающая хранение, обработку, преобразование и передачу информации администрации с использованием компьютерной и другой техники (далее – ИСПДн);

администратор ИСПДн – гражданский служащий или работник, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения (далее – ПО) и оборудования вычислительной техники. Ответственный за администрирование информационных систем персональных данных;

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);

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 ИСПДн понимается их подключение к инфраструктуре ИСПДн с целью обработки, приема/передачи информации между ИСПДн 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 разрешается только пользователям, имеющим разрешение на предоставление доступа к сменным носителям в режиме записи (далее – разрешение).

3.4. Разрешение осуществляется администратором ИСПДн по заявкам руководителей структурных подразделений администрации.

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. Передача заявки в отдел информационных технологий для выполнения технических настроек.

3.5.3. Отдел информационных технологий предоставляет разрешение или отказывает в предоставлении разрешения.

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 администратора ИСПДн о любых фактах нарушения требований настоящего регламента.

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

3.6.5. Извещать администраторов ИСПДн 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 ИСПДн администрации.

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

3.10. При возникновении подозрений в отношении пользователя 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 2
к приказу администрации Губернатора
Брянской области и Правительства
Брянской области
от 6 мая 2024 г. № 230-пр

«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).

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

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

Администратор безопасности – гражданский служащий или работник, обеспечивающий ввод в эксплуатацию, поддержку и последующий вывод из эксплуатации программного обеспечения (далее – ПО) и оборудования вычислительной техники. Лицо, ответственное за информационную безопасность;

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);

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 администрации понимается их подключение к АРМ с целью обработки, приема/передачи информации между АРМ и носителями информации.

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

3.3. При использовании пользователями сменных носителей информации необходимо:

3.3.1. Соблюдать требования настоящего регламента.

3.3.2. Использовать носители информации исключительно для выполнения служебных обязанностей.

3.3.3. Ставить в известность администраторов безопасности о любых фактах нарушения требований настоящего регламента.

3.3.4. Извещать администраторов безопасности о фактах утраты (кражи) сменных носителей информации.

3.4. При использовании пользователями сменных носителей информации запрещено:

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

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

3.5. Администрация оставляет за собой право блокировать или ограничивать использование сменных носителей информации на АРМ администрации.

3.6. При возникновении подозрений в отношении пользователя о несанкционированном и/или нецелевом использовании сменных носителей информации инициируется проведение служебной проверки в соответствии с действующим законодательством.

3.7. 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 3
к приказу администрации Губернатора
Брянской области и Правительства
Брянской области
от 6 мая 2024 г. № 230-пр

«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 предназначена для государственных гражданских служащих Брянской области, замещающих должности государственной гражданской службы Брянской области в администрации Губернатора Брянской области и Правительства Брянской области (далее – администрация), и работников администрации, замещающих должности, не являющиеся должностями государственной гражданской службы Брянской области (далее – пользователи).

2. Настоящая Инструкция регламентирует организационно-техническое обеспечение процессов генерации, смены и прекращения действия паролей (блокирование или удаления учетных записей пользователей) на автоматизированных рабочих местах администрации.

3. Первоначальные пароли доступа выдаются пользователям лицом, ответственным за информационную безопасность (далее – администратор безопасности). При первом входе в систему происходит запрос нового пароля пользователя, соответствующего правилам формирования паролей.

4. Правила формирования пароля:

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

пароль должен состоять не менее чем из 12 символов;

в числе символов пароля обязательно должны присутствовать символы трех категорий из числа следующих четырех:

а) прописные буквы английского алфавита от A до Z;

б) строчные буквы английского алфавита от a до z;

в) десятичные цифры (от 0 до 9);

г) специальные символы, не принадлежащие алфавитно-цифровому набору (@, #, $, &, *, % и т.п.);

запрещается использовать в качестве пароля имя входа в систему простые пароли типа «123», «111», «qwerty», «zxcvb», «qazxswedc» и им подобные, а также свое имя и дату рождения, имена и даты рождения 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 (1234567, qwerty и т.п.);

при смене пароля новое значение должно отличаться от предыдущего не менее чем в четырех позициях;

запрещается выбирать пароли, которые уже использовались ранее;

личный пароль пользователь не имеет права никому сообщать;

периодичность смены пароля определяется принятой политикой безопасности, но не должна превышать 90 календарных дней.

5. Количество неудачных попыток входа в систему, приводящее к блокировке учетной записи пользователя, должно быть не более трех. Разблокирование учетной записи и сброс пароля на первоначальный осуществляется администраторами безопасности.

6. После 15 минут бездействия (неактивности) пользователя должно происходить автоматическое блокирование сеанса доступа. Блокирование сеанса доступа пользователя в операционную систему должно сохраняться до прохождения им повторной идентификации и аутентификации.

7. Порядок смены пароля:

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

полная внеплановая смена паролей должна производиться в случае компрометации личного пароля администратора или администраторов безопасности;

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 хранение пароля:

запрещается записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

запрещается сообщать другим пользователям личный пароль и регистрировать их в системе под своим паролем.

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 администратору безопасности, администраторам об утере, компрометации, несанкционированном изменении паролей и несанкционированном изменении сроков действия паролей.»