МІНІСТЭРСТВА АХОВЫ ЗДАРОЎЯ РЭСПУБЛІКІ БЕЛАРУСЬ

ЗАГАД

03.01.2025 № 3

г. Мінск

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

ПРИКАЗ

г. Минск

Об установлении Примерного регламента организации доступа к объектам информационной инфраструктуры

На основании абзаца седьмого части третьей статьи 8 Закона Республики Беларусь от 18 июня 1993 г. № 2435-XII «О здравоохранении», подпункта 9.1 пункта 9 Положения о Министерстве здравоохранения Республики Беларусь, утвержденного постановлением Совета Министров Республики Беларусь от 28 октября 2011 г. № 1446,
ПРИКАЗЫВАЮ:

1. Установить Примерный регламент организации доступа к объектам информационной инфраструктуры (прилагается).

2. Руководителям организаций государственной системы здравоохранения принять меры по реализации настоящего приказа.

3. Контроль за исполнением настоящего приказа возложить на заместителя Министра здравоохранения Андросюка Б.Н.

Министр А.В.Ходжаев

УТВЕРЖДЕНО
Приказ
Министерства здравоохранения
Республики Беларусь
03.01.2025 № 3

ПРИМЕРНЫЙ РЕГЛАМЕНТ
организации доступа к объектам информационной инфраструктуры

ГЛАВА 1
ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

1. В Настоящем Примерном регламенте применяются следующие термины и их определения, сокращения:

административные права доступа – особые привилегии учетной записи, предоставляющие полный доступ к объектам информационной инфраструктуры организации здравоохранения и возможность изменения прав доступа других пользователей;

доступ к объектам – получение и реализация субъектом прав на выполнение определенных действий (чтение, выполнение, запись, изменение, удаление и т.д.) по отношению к объекту ИИ ОЗ;

зона безопасности – помещение (помещения) с особым режимом контролируемого доступа ограниченного круга лиц, который поддерживается в целях обеспечения защиты активов ОЗ;

инициатор договора – инициатор заключения гражданско-правового договора на выполнение работ (оказание услуг);

корпоративная сеть – совокупность средств вычислительной техники (персональных компьютеров, серверов, периферийного оборудования и т.д.), соединенных линиями связи, образованная коммуникационным оборудованием;

парольная политика – набор правил, определяющих сложность паролей, и ограничений на использование паролей в информационной системе (ресурсе);

подрядчик – физическое лицо, с которым ОЗ заключен гражданско-правовой договор на выполнение работ (оказание услуг);

права доступа – совокупность правил и политик, определяющих условия и порядок доступа к объектам ИИ ОЗ;

представитель сторонней организации – работник (уполномоченный представитель) сторонней организации, с которым ОЗ заключен гражданско-правовой договор на выполнение работ (оказание услуг);

регистрационные данные – сведения о субъекте, необходимые для предоставления доступа к объектам ИИ ОЗ*;

сторонняя организация – организация, выполняющая работы (оказывающая услуги) для ОЗ и (или) взаимодействующая с информационными ресурсами ОЗ посредством своих работников (уполномоченных представителей) и (или) вычислительных процессов;

субъект – работник ОЗ, физическое лицо, работник (уполномоченный представитель) сторонней организации или индивидуальный предприниматель, с которым (которой) ОЗ заключен гражданско-правовой договор на выполнение работ (оказание услуг), получивший в установленном порядке доступ к объектам ИИ ОЗ;

учетная запись – логический объект, существующий в пределах одной или нескольких информационных систем (ресурсов) и представляющий субъекта в ее (их) пределах;

ОЗ – организация здравоохранения;

ЗИ – защита информации;

ИБ – информационная безопасность;

ИИ – информационная инфраструктура;

ОС – операционная система;

ПК – персональный компьютер;

ПО – программное обеспечение;

СНИ – съемный носитель информации.

---

*Для целей настоящего Примерного регламента под сведениями понимаются:

в отношении работников ОЗ:

фамилия, собственное имя, отчество (если таковое имеется), дата рождения, наименование структурного подразделения (при наличии), занимаемая должность, дата трудоустройства работника, номер мобильного телефона при наличии соответствующего согласия на обработку персональных данных;

в отношении физического лица, с которым ОЗ заключен гражданско-правовой договор на выполнение работ (оказание услуг):

фамилия, собственное имя, отчество (если таковое имеется), дата рождения, номер мобильного телефона, дата заключения договора с подрядчиком, сроки выполнения работы (оказания услуг), фамилия, собственное имя, отчество (если таковое имеется) и должность ответственного лица ОЗ, который курирует деятельность подрядчика.

ГЛАВА 2
ОБЩИЕ ПОЛОЖЕНИЯ

2. Настоящий Примерный регламент применяется при организации доступа к объектам ИИ ОЗ и определяет порядок управления доступом субъектов к объектам ИИ.

3. Объекты ИИ и средства связи должны использоваться субъектами исключительно в служебных целях.

4. Управление доступом к объектам информационных систем, собственником, владельцем и (или) оператором которых является ОЗ и которые не входят в состав ИИ ОЗ, регламентируется отдельными локальными актами ОЗ.

5. Доступ к объектам ИИ ОЗ и выполнению операций над объектами должен предоставляться только идентифицированным субъектам. Блок-схемы процессов предоставления, прекращения и изменения прав доступа работников к объектам ИИ ОЗ приведены в приложениях 1–4.

6. Подразделение защиты информации или иное подразделение (должностное лицо), ответственное за обеспечение защиты информации (далее – ОИБ), обеспечивает ознакомление субъектов в части их касающейся с локальными актами в области информационной безопасности ОЗ.

7. Лицо, назначенное в ОЗ ответственным за осуществление внутреннего контроля за обработкой персональных данных, обеспечивает ознакомление субъектов в части их касающейся с локальными актами ОЗ в области защиты персональных данных.

8. На период отсутствия уполномоченного должностного лица его функции возлагаются на лицо, исполняющее его обязанности.

9. Работники ОЗ вправе запрашивать у заинтересованных сторон дополнительные сведения, необходимые для корректного выполнения своих обязанностей, предусмотренных Примерным регламентом.

10. Примерный регламент разработан в соответствии с требованиями приказа Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449».

11. Примерный регламент разработан в соответствии с требованиями следующих технических нормативных правовых актов в области технического нормирования и стандартизации:

ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements;

СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

ГЛАВА 3
ПРЕДОСТАВЛЕНИЕ ДОСТУПА РАБОТНИКАМ И ПОДРЯДЧИКАМ К ОБЪЕКТАМ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

12. В целях своевременной подготовки рабочих мест подразделение по учету кадров или иное подразделение (должностное лицо), ответственное за учет кадров (инициатор договора) (далее – ОК) уведомляет подразделение по информационным технологиям или иное подразделение (должностное лицо), ответственное за информатизацию (далее – ОИТ) ОЗ и ОИБ ОЗ о предстоящем трудоустройстве работника (заключении договора с подрядчиком) не позднее пяти рабочих дней до дня начала деятельности субъектом.

13. ОИТ ОЗ выполняет первоначальную подготовку и настройку рабочего места субъекта (ПК и (или) мобильного технического средства, рабочего телефона), установку ПО, входящего в состав типового рабочего места.

14. Для установки и начальной настройки ОС используется локальная учетная запись администратора. Для локальной учетной записи администратора должен быть задан пароль, соответствующий следующим требованиям:

состоит не менее чем из восьми символов;

не содержит последовательность одинаковых цифр или букв, имя учетной записи или какую-либо его часть;

содержит символы трех категорий из числа следующих:

буквы верхнего регистра;

буквы нижнего регистра;

цифры;

специальные символы.

15. ОИБ ОЗ обеспечивает ввод ПК работника в корпоративный домен после завершения начальной настройки ОС.

16. Доступ к локальной учетной записи администратора должен быть ограничен и использоваться исключительно для служебных нужд ОИТ и ОИБ ОЗ.

17. Типовые права доступа к объектам ИИ ОЗ предоставляются работнику (подрядчику) не позднее рабочего дня, следующего за днем трудоустройства (заключения договора). Основанием является заявка на предоставление доступа по форме, указанной в приложении 5.

18. Предоставление доступа инициируется:

ОК – в отношении работников ОЗ;

инициатором договора – в отношении подрядчиков ОЗ.

19. При инициировании предоставления доступа должны быть представлены:

заявка на предоставление доступа с указанием регистрационных данных;

копия согласия на обработку персональных данных по форме согласно Политике ОЗ в отношении обработки персональных данных в процессе трудовой деятельности и при осуществлении административных процедур.

20. Заявки на предоставление (прекращение, изменение) доступа подлежат учету.

21. Руководитель структурного подразделения, в состав которого входит субъект, или должностное лицо, в подчинении которого находится субъект, должен определить необходимость предоставления субъекту дополнительных прав доступа.

22. Впоследствии работник может изменять ранее предоставленный набор прав доступа, повторно отправляя и согласовывая соответствующие заявки. Изменение прав доступа подрядчика должно инициировать лицо, которое курирует его деятельность.

23. В случае отсутствия оснований для предоставления доступа и (или) некорректного оформления заявки доступ не предоставляется.

24. Предоставление субъекту прав доступа реализуется последовательно:

ОИТ ОЗ в части:

предоставления типовых прав доступа к:

корпоративной сети;

электронной почте;

файловому хранилищу;

системе электронного документооборота;

корпоративному порталу (при наличии);

медицинский информационной системе (при наличии);

ПО, входящему в состав типового рабочего места;

предоставления дополнительных прав доступа.

ОИБ ОЗ в части установки и настройки необходимых средств ЗИ (антивирусного ПО, средств сбора событий ИБ, средств криптографической ЗИ), предоставления доступа в сеть Интернет, обновления списка разрешенных устройств.

25. ОИТ ОЗ создает для субъекта персональную, доменную учетную запись с активным параметром необходимости смены пароля при первом входе.

26. При создании учетной записи должны быть заполнены пользовательские атрибуты, отражающие регистрационные данные.

27. Парольная политика для учетной записи должна соответствовать следующим требованиям:

максимальный срок использования пароля – 180 дней, минимальный срок действия пароля – 0 дней, повторяемость – последние 5 паролей не должны совпадать;

пароль должен соответствовать следующим требованиям:

состоит не менее чем из восьми символов;

не содержит последовательность одинаковых цифр или букв, имя учетной записи или какую-либо его часть;

содержит символы трех категорий из числа следующих:

буквы верхнего регистра английского или русского алфавита;

буквы нижнего регистра английского или русского алфавита;

цифры;

специальные символы (например: !, $, #, %).

В случае регистрации трех неудачных попыток входа в учетную запись должно выполняться блокирование учетной записи на 15 минут до ее автоматического разблокирования. Блокирование активного сеанса субъекта должно выполняться после 15 минут бездействия, при активации (разблокировке) необходимо требовать ввод пароля.

28. Администраторы ресурса обеспечивают создание персональных учетных записей для доступа субъектов к необходимым им информационным ресурсам и сервисам ОЗ. Парольная политика для таких учетных записей должна соответствовать требованиям пункта 28 Примерного регламента (при наличии технических возможностей) или согласовываться с ОИБ ОЗ.

29. Для использования объектов ИИ ОЗ субъект должен получать минимальный набор прав доступа, необходимый для выполнения должностных обязанностей. Доступ должен предоставляться только идентифицированным устройствам и субъектам. Для этого должны применяться следующие основные механизмы безопасности:

ограничение прав доступа к файловой системе и ресурсам ОС;

контроль и ограничение запуска исполняемых файлов и приложений в соответствии с белым списком;

контроль и ограничение подключения к ПК внешних устройств и использования СНИ (USB Flash, USB HDD, CD, DVD и т.д.) в соответствии с белым списком;

контроль и ограничение доступа к корпоративной сети и сетевым ресурсам.

30. Для управления и организации доступа субъектов к объектам ИИ ОЗ используются доменные и локальные учетные записи. Встроенные локальные учетные записи с административными привилегиями на каждом ПК, мобильном рабочем месте и сервере, должны быть отключены.

31. Использование административных учетных записей допускается только для выполнения должностных обязанностей.

Для администрирования доменных объектов должна применяться гранулированная политика паролей с разделением привилегированных и пользовательских учетных записей.

32. Административные права доступа подлежат учету, ОТ ОЗ должен вести (в электронном виде) журнал учета таких прав, содержащий следующую информацию: объект доступа, факторы аутентификации, категория учетной записи, фамилия, собственное имя, отчество (если таковое имеется) и должность допущенного.

33. Не допускается использование реквизитов доступа, установленных производителем по умолчанию.

34. В случае компрометации реквизитов доступа должна производится их смена или блокирование.

35. Разрешенное к использованию ПО определяется в перечне разрешенного ПО, ответственность за ведение которого возлагается на ОИБ ОЗ.

36. Разрешенное ПО, входящее в состав типового рабочего места, устанавливается на ПК по умолчанию в ходе первоначальной подготовки и настройки рабочего места субъекта.

37. Установка ПО, не входящего в состав типового рабочего места, осуществляется только после предоставления субъектом или его непосредственным руководителем соответствующей заявки. В случае согласования ОИБ ОЗ актуализирует перечень разрешенного ПО, после чего ОИТ ОЗ проводит установку необходимого ПО.

При отсутствии необходимого ПО в ресурсах ОЗ непосредственный руководитель субъекта готовит докладную записку на приобретение ПО в установленном порядке.

До начала инсталляции обязательно выполнение антивирусной проверки файлов дистрибутивов.

В случае окончания лицензионного срока использования ПО, вывода из эксплуатации или замены на альтернативное ОИТ ОЗ удаляет его со всех объектов ИИ ОЗ.

38. Контроль и ограничение запуска исполняемых файлов и приложений выполняется средством защиты конечных устройств в соответствии с белым списком. Настройку модуля контроля приложений и поддержание белого списка в актуальном состоянии выполняет ОИБ ОЗ.

39. ОИТ ОЗ обязан вести (в электронном виде) и поддерживать в актуальном состоянии реестр информационных ресурсов и сервисов ОЗ с указанием лиц, ответственных за их администрирование (администраторов ресурса).

40. ОИБ и ОИТ ОЗ в рамках выполнения своих должностных обязанностей имеют право на полный доступ к корпоративной сети ОЗ, ПК и мобильным рабочим местам без уведомления субъектов.

При подключении к удаленному рабочему столу ПК субъектов должен выводиться запрос на подключение. Работы при таком подключении могут выполняться при согласии субъекта.

ОИБ и ОИТ ОЗ с целью повышения уровня безопасности объектов ИИ ОЗ имеют право без уведомления субъектов производить работы по инсталляции дополнительного ПО на ПК и мобильные рабочие места субъектов, проводить плановые и внеплановые сканирования на отсутствие вредоносного ПО, осуществлять иную деятельность в соответствии со своими функциями.

По решению руководителя ОЗ либо его заместителя, курирующего вопросы информационных технологий или вопросы ИБ, ОИБ и ОИТ ОЗ вправе использовать программные и программно-технические средства контроля за надлежащим исполнением работниками своих должностных обязанностей и осуществлять мониторинг информации, обрабатываемой в ИИ.

41. ОИТ ОЗ должен ознакомить субъекта с реквизитами доступа и предоставленными ему правами доступа.

42. В день трудоустройства (после оформления кадровых документов) или после заключения договора с подрядчиком ОК или инициатор договора (при наличии такой необходимости) должен уведомить руководителя ОИТ ОЗ о прибытии субъекта и направить его в ОИТ для регистрации в системе контроля и управления доступом (при наличии) и оформления постоянного пропуска.

Порядок изготовления и выдачи электронных пропусков, а также получения (при наличии соответствующего согласия на обработку персональных данных) биометрических данных субъекта для внесения в терминалы доступа определяется Положением о пропускном и внутриобъектовым режиме в ОЗ, утверждаемым руководителем ОЗ.

ГЛАВА 4
ПРЕКРАЩЕНИЕ ДОСТУПА РАБОТНИКА ИЛИ ПОДРЯДЧИКА К ОБЪЕКТАМ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

43. Прекращение доступа к объектам ИИ ОЗ осуществляется:
в случае кадровых событий:
увольнением работника;
окончанием срока действия (расторжением) договора с подрядчиком;
предоставлением отпуска по уходу за ребенком в возрасте до трех лет;

иными обстоятельствами, не зависящими от воли сторон, – в последний рабочий день субъекта, если не определено иное;

в случае, если субъект в течение двух месяцев не осуществлял вход под своей учетной записью на объекты ИИ;

в случае решения ОИТ и (или) ОИБ ОЗ об ограничении предоставляемого доступа субъекту (при попытках нецелевого использования объектов, предоставляемых прав доступа, инцидентах ИБ);

в случае решения руководителя ОЗ или его заместителя, курирующего вопросы информационных технологий или вопросы ИБ.

44. Прекращение доступа инициируется:

ОК – в отношении работников ОЗ;

инициатором договора – в отношении подрядчиков ОЗ.

45. ОК или инициатором договора оформляется заявка на прекращение доступа, согласно приложению 6 к настоящему Примерному регламенту.

46. Руководитель структурного подразделения, в состав которого входит субъект, или должностное лицо, в подчинении которого находится субъект, в случае служебной необходимости может оформить запрос на сохранение доступа к учетным записям субъекта, его почтовому ящику и т.п. посредством заявки на прекращение доступа.

47. В случае отсутствия в заявке периода времени, в течение которого необходимо сохранить доступ к данным субъекта, а также при необоснованности такого запроса, запрос не удовлетворяется.

48. Прекращение доступа к объектам ИИ ОЗ осуществляется ОИТ, ОИБ ОЗ и администраторами ресурса не позднее времени окончания рабочего дня даты прекращения доступа, и включает следующие этапы:

отключение учетной записи субъекта на срок до 30 дней и ее удаление по истечении указанного срока (если не определено иное заявкой);

изменение конфигурации ресурсов и прав доступа;

изъятие служебного СНИ;

передача служебного СНИ руководителю указанного работника для анализа на предмет наличия конфиденциальной информации, информации, распространение и (или) предоставление которой ограничено, иной информации, необходимой для выполнения целей и задач ОЗ и последующее форматирование СНИ для передачи другому работнику (при необходимости).

49. ОИБ ОЗ должен осуществлять проверку действующих учетных записей субъектов.

50. ОИБ ОЗ осуществляет информирование увольняемого работника (подрядчика, заключенный договор с которым истек (расторгнут)) по вопросам ЗИ, распространение и (или) предоставление которой ограничено (собственником которой является ОЗ).

ГЛАВА 5
ИЗМЕНЕНИЕ УЧЕТНЫХ ЗАПИСЕЙ РАБОТНИКОВ ИЛИ ПОДРЯДЧИКОВ И ПРАВ ДОСТУПА К ОБЪЕКТАМ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

51. Изменение учетных записей субъекта и прав доступа к объектам ИИ ОЗ осуществляется:

в случае кадровых событий:

перевод работника в другое структурное подразделение;

назначение работника на новую должность;

переводом работника на другую работу для замещения временно отсутствующего работника;

на основании заявки работника на предоставление доступа при необходимости получения дополнительных прав доступа;

на основании заявки ответственного лица, который курирует деятельность подрядчика, на предоставление доступа при необходимости получения дополнительных прав доступа;

в случае решения ОИТ и ОИБ ОЗ об ограничении предоставляемого доступа субъекту (при попытках нецелевого использования объектов, предоставляемых прав доступа; инцидентах ИБ);

в случае распоряжения руководителя ОЗ или его заместителя, курирующего вопросы информационных технологий или вопросы ИБ.

52. ОК не позднее чем за один рабочий день до наступления соответствующего кадрового события должен уведомить:

руководителя структурного подразделения, в состав которого войдет субъект, или должностное лицо, в подчинении которого будет находиться субъект;

руководителя ОИБ ОЗ.

53. Уведомление осуществляется по форме приведенной в приложении 7 к настоящему Примерному регламенту.

54. Изменение учетных записей субъектов и прав доступа к объектам ИИ ОЗ осуществляется ОИТ, ОИБ, администраторами ресурса и включает:

отключение локальной учетной записи субъекта для конкретного ресурса;

изменение конфигурации ресурсов и прав доступа.

55. ОИБ осуществляет информирование переводимого работника по вопросам ЗИ, распространение и (или) предоставление которой ограничено.

ГЛАВА 6
ПРЕДОСТАВЛЕНИЕ И ПРЕКРАЩЕНИЕ ДОСТУПА ПРЕДСТАВИТЕЛЯМ СТОРОННИХ ОРГАНИЗАЦИЙ, ИНДИВИДУАЛЬНЫМ ПРЕПРИНИМАТЕЛЯМ К ОБЪЕКТАМ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

56. Основанием для предоставления доступа к объектам ИИ ОЗ представителям сторонней организации, индивидуальным предпринимателям является договор (соглашение о взаимодействии) между ОЗ и соответствующей сторонней организацией, индивидуальным предпринимателем или докладная записка, согласованная руководителем ОЗ.

57. Договор (соглашение о взаимодействии, докладная записка) должен содержать:

наименование сторонней организации (фамилию, собственное имя, отчество (если таковое имеется) индивидуального предпринимателя);

срок выполнения работ (оказания услуг) и (или) дату окончания действия договора (соглашения о взаимодействии);

сведения о представителях сторонних организаций, индивидуальном предпринимателе, которым необходимо получить доступ, и технических специалистах (фамилия, собственное имя, отчество (если таковое имеется), должность (при наличии), структурное подразделение (при наличии), контактный телефон, электронная почта;

наименование ресурсов, сервисов или их компонентов, к которым необходимо получить доступ;

права доступа и тип подключения к ресурсам, сервисам или их компонентам.

58. Предоставляемые права доступа должны соответствовать функциям, которые данная организация или индивидуальный предприниматель выполняет в рамках исполнения обязательств по договору (соглашению о взаимодействии).

59. Период предоставления доступа представителю сторонней организации (индивидуальному предпринимателю) к объектам ИИ ОЗ не должен превышать периода действия договора (соглашения о взаимодействии).

60. Договор (соглашение о взаимодействии) также должен содержать обязательства сторонней организации по:

обеспечению ЗИ, распространение и (или) предоставление которой ограничено, обрабатываемой при исполнении договора (соглашения о взаимодействии);

незамедлительному информированию ОЗ о допущенном представителем сторонней организацией, индивидуальным

предпринимателем или ставшем ему известным факте компрометации, разглашения или об угрозе разглашения, о незаконном получении или незаконном использовании третьими лицами информации, распространение и (или) предоставление которой ограничено.

61. В рамках оказания услуг с представителями сторонних организаций, индивидуальными предпринимателями необходимо заключать договор (соглашение) о неразглашении конфиденциальной информации и ответственности за ее разглашение, если такие условия не предусматривает заключенный договор (соглашение о взаимодействии).

62. Проекты договоров (соглашений о взаимодействии), предполагающие предоставление доступа к объектам ИИ ОЗ представителям сторонних организаций, индивидуальным предпринимателям и договоры о неразглашении конфиденциальной информации подлежат согласованию с руководителями ОИБ и ОИТ ОЗ.

63. Ответственный исполнитель по договору (соглашению о взаимодействии) не позднее чем, за один рабочий день до начала работ, должен уведомить руководителя ОИБ.

64. Структурное подразделение ОЗ, курирующее выполнение работ (оказание услуг) сторонней организацией, индивидуальным предпринимателем должно ознакомить представителей сторонней организации, индивидуального предпринимателя с действующими правилами ИБ либо направить их в ОИБ для проведения соответствующего инструктажа.

65. Основанием для прекращения доступа представителям сторонней организации, индивидуального предпринимателя к объектам ИИ ОЗ могут быть:

прекращение срока действия договора (соглашения о взаимодействии), по которому был получен доступ;

извещение сторонней организации, индивидуального предпринимателя о необходимости прекращения доступа;

окончание срока предоставления прав доступа;

решение ОИТ и (или) ОИБ об ограничении предоставляемого доступа субъектам при попытках нецелевого использования объектов, предоставляемых прав доступа и (или) инцидентах ИБ;

решение руководителя ОЗ.

66. Доступ к объектам ИИ ОЗ в целях проведения наладочных работ и сервисного обслуживания должен предоставляться третьим лицам только при совокупном соблюдении следующих условий:

при наличии договора (соглашения) о конфиденциальности;

при наличии договора (соглашения) о проведении работ;

участия ОИБ.

ГЛАВА 7
ПОРЯДОК УДАЛЕННОЙ РАБОТЫ С ОБЪЕКТАМИ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

67. Субъекты в соответствии со своими должностными обязанностями (или во исполнение договорных обязательств) и в случае производственной необходимости могут удаленно подключаться к объектам ИИ ОЗ.

68. Предоставление удаленного доступа к объектам ИИ ОЗ осуществляется на основании оформленной и согласованной заявки.

69. Организацию удаленных подключений субъектов к объектам ИИ ОЗ, а именно процедуры настройки средств межсетевого экранирования, построение защищенных туннелей осуществляют ОИТ и ОИБ в части их касающейся.

70. При организации удаленного подключения к объектам ИИ ОЗ представителей сторонних организаций, индивидуальных предпринимателей, подрядчиков должен быть разрешен доступ только к объектам, предусмотренным договором (соглашением о взаимодействии).

ГЛАВА 8
ПОРЯДОК ИСПОЛЬЗОВАНИЯ МОБИЛЬНЫХ ТЕХНИЧЕСКИХ СРЕДСТВ И СЪЕМНЫХ НОСИТЕЛЕЙ ИНФОРМАЦИИ

71. Под использованием мобильных технических средств и СНИ понимается их подключение к ИИ ОЗ с целью передачи, хранения и обработки информации.

72. Разрешается подключение к объектам ИИ ОЗ только учтенных СНИ. В случае необходимости субъекту может быть выдан служебный СНИ для подключения к ИИ ОЗ.

73. Для учета разрешенных СНИ и контроля их подключения к объектам ИИ используются функции средства защиты конечных устройств.

74. Настройку средств защиты конечных устройств выполняет ОИБ. При добавлении СНИ в список доверенных должны быть заданы дата добавления устройства и учетная запись субъекта, которому разрешено подключение конкретного СНИ. Также средство защиты конечных устройств должно регистрировать события о записи файлов на СНИ.

75. Субъектам запрещается использовать служебные СНИ в личных целях.

76. Обработка (копирование, исполнение) файлов, переносимых на СНИ, должна производиться при включенном средстве антивирусной защиты.

77. На всех ПК, мобильных технических средствах и серверах из состава ИИ ОЗ необходимо отключить функции автозагрузки СНИ при их подключении.

78. В случае присутствия на СНИ неизвестных файлов, открытие таких файлов запрещается.

79. Ответственность за сохранность СНИ, а также за утечку информации, распространение и (или) предоставление которой ограничено, записанной на СНИ, несет субъект, за которым закреплен данный носитель.

80. О случаях утраты, порчи СНИ, а также о возникновении ситуаций, которые могут к ним привести, субъекты должны немедленно информировать ОИБ.

81. Контроль за использованием СНИ, организация работ по уничтожению или форматированию служебных СНИ возлагается на ОИБ.

82. Запрещено подключение любых мобильных технических средств (за исключением служебных) к корпоративной сети ОЗ.

ГЛАВА 9
ПОРЯДОК РАБОТЫ В ЗОНЕ БЕЗОПАСНОСТИ

83. Право доступа в зону безопасности (серверное помещение) предоставлено руководителю ОЗ, его заместителю, курирующего вопросы информационных технологий или вопросы ИБ, руководителю ОИБ, руководителю ОИТ, работникам ОИТ (согласно должностным обязанностям). Доступ иных лиц в зону безопасности осуществляется в сопровождении лиц, указанных выше.

84. Ключи для доступа в зону безопасности и их дубликаты должны храниться у начальника ОИТ. При необходимости доступ может контролироваться с использованием системы контроля и управления доступом.

ГЛАВА 10
ОТВЕТСТВЕННОСТЬ

85. Субъекты несут ответственность за выполнение требований настоящего регламента и должностных обязанностей в части организации и соблюдения порядка доступа.

86. С целью минимизирования возможности возникновения инцидентов ИБ субъекты должны следовать политикам «чистого стола» и «чистого экрана»:

интерактивные сеансы при работе с ПК и мобильным техническим средством должны быть блокированы в случае отсутствия субъекта;

все бумажные документы, содержащие информацию, распространение и (или) предоставление которой ограничено, СНИ, средства формирования и проверки электронной цифровой подписи должны находиться под присмотром или быть убраны в запираемые ящики стола, шкаф, сейф и т.п.;

носители информации, распространение и (или) предоставление которой ограничено, СНИ, средства формирования и проверки электронной цифровой подписи должны храниться в шкафах и (или) других запираемых предметах мебели;

запираемые места хранения (ящики столов, шкафы, сейфы) при оставлении рабочего места должны быть закрыты;

файлы, отправленные на печать, не должны оставаться в лотке выдачи принтеров, многофункциональных устройств;

после совершения операций сканирования или ксерокопирования необходимо проверять лоток сканера или ксерокса, чтобы убедиться, что документ, с которого изготавливаются копии, изъят.

87. После получения доступа к объектам ИИ ОЗ субъектам запрещается:

несанкционированное подключение к объектам ИИ СНИ и мобильных технических средств;

сообщать иным лицам свои реквизиты доступа к объектам ИИ ОЗ, а также осуществлять рабочую деятельность от имени другого субъекта;

передавать средства формирования и выработки электронной цифровой подписи третьим лицам, использовать скомпрометированную ключевую информацию или ключевую информацию, срок действия которой истек;

хранение реквизитов доступа в открытом виде и в общедоступных местах;

производить вскрытие вычислительной техники, входящей в состав ИИ ОЗ;

удалять информацию, которая относится к рабочей деятельности и может представлять потенциальную пользу или ценность для ОЗ, без согласования со своим непосредственным руководителем;

сообщать личные номера телефонов или иные личные данные других работников третьим лицам без предварительного согласования;

разглашать ставшую известной в ходе рабочей деятельности информацию, распространение и (или) предоставление которой ограничено, в том числе касающуюся ИИ ОЗ.

88. ОК (инициатор договора) обязан предоставлять список работников (подрядчиков) ОЗ по запросу руководителей ОИТ и ОИБ либо по запросу работников ОИТ и ОИБ при наличии согласования с их руководителем, подтверждающего полномочия работника на получение

информации. Запрос и ответ на него должны направляться посредством корпоративной электронной почты или корпоративного портала.

Предоставляемые сведения:

о работниках:

фамилия, собственное имя, отчество (если таковое имеется);

структурное подразделение (при наличии);

должность;

дату трудоустройства;

дату увольнения (при наличии);

иные сведения, определенные запросом (при необходимости);

о подрядчиках:

фамилия, собственное имя, отчество (если таковое имеется);

наименование выполняемых работ (оказываемых услуг);

дату заключения договора;

дату прекращения договора (при наличии);

сроки выполнения работы (оказания услуг);

иные сведения, определенные запросом (при необходимости).

Предоставление сведений осуществляется не позднее одного рабочего дня со дня поступления запроса.

89. В случае подозрения на несанкционированный доступ к объектам ИИ ОЗ, нестандартное поведение системного и прикладного ПО, возможную компрометацию аутентификационных и идентификационных данных, возникновение инцидента ИБ, субъекты обязаны прекратить процедуры обработки (приема-передачи) информации на соответствующих объектах, незамедлительно информировать об этом ОИБ и (или) ОИТ.

90. Представители сторонних организаций, индивидуальные предприниматели и подрядчики, уполномоченные на получение доступа к объектам ИИ ОЗ, несут персональную ответственность за нарушение требований ИБ и могут быть привлечены к ответственности в соответствии с договором (соглашением о взаимодействии) и законодательством.

Приложение 1
к Примерному регламенту организации доступа к объектам информационной инфраструктуры

БЛОК-СХЕМА
процесса предоставления доступа к объектам информационной инфраструктуры

Шаг	Исполнитель	Результат
1	ОК (инициатор договора)	Поставлена задача для предоставления субъекту типовых прав доступа к объектам ИИ ОЗ. Представлена заполненная заявка на предоставление доступа.
2.1	Руководитель структурного подразделения (инициатор договора)	Определена необходимость предоставления субъекту дополнительных прав доступа к объектам ИИ ОЗ. При отсутствии такой необходимости задача исполнена.
2.2		Заполнены соответствующие поля заявки на предоставление доступа (при необходимости предоставления субъекту дополнительных прав доступа).
3.1	ОИБ	Согласовано предоставление субъекту типовых прав доступа к объектам ИИ ОЗ. Соисполнителю (ОИТ) поставлена подзадача предоставления субъекту типового набора прав доступа к объектам ИИ ОЗ.
3.2		Согласовано предоставление субъекту дополнительных прав доступа к объектам ИИ ОЗ. Соисполнителю (ОИТ) поставлена подзадача предоставления субъекту типовых и дополнительных прав доступа к объектам ИИ ОЗ.
4.1	ОИТ	Согласовано предоставление субъекту типовых прав доступа к объектам ИИ ОЗ. Сформирована учетная запись с заполнением атрибутов субъекта и назначением временного пароля. Субъекту предоставлен доступ к типовому комплекту

Шаг	Исполнитель	Результат
		информационных ресурсов (доступ к корпоративной сети, электронной почте, файловому хранилищу, системе электронного документооборота, корпоративному порталу, медицинской информационной системе). Сведения, содержащие сетевое имя устройства, имя учетной записи в Active Directory и имя почтовой учетной записи субъекта, предоставлены в качестве результата исполнения задачи.
4.2	ОИТ	Согласовано предоставление субъекту дополнительных прав доступа к объектам ИИ ОЗ. Определена необходимость предоставления доступа к информационным ресурсам и сервисам ОЗ не своей зоны ответственности. Сформирована учетная запись с заполнением атрибутов субъекта и назначением временного пароля. Субъекту предоставлен доступ к типовому и дополнительному комплекту информационных ресурсов согласно заявке. Сведения, содержащие сетевое имя устройства, имя учетной записи в Active Directory и имя почтовой учетной записи субъекта, предоставлены в качестве результата исполнения задачи.
4.3		Соисполнителю (администратору ресурса) поставлена подзадача для предоставления субъекту дополнительных прав доступа к объектам ИИ ОЗ (информационным ресурсам и сервисам ОЗ).
4.4	Администратор ресурса	Предоставлен доступ к информационным ресурсам и сервисам своей зоны ответственности.
5	ОИБ	На рабочем месте субъекта установлены и настроены необходимые средства ЗИ (антивирусное ПО, средства сбора событий ИБ), предоставлен доступ в сеть Интернет.
		Внешние устройства для подключения к ПК внесены в список разрешенных устройств. Установлены и настроены средства криптографической ЗИ (при необходимости организации удаленного защищенного канала передачи данных).

Приложение 2
к Примерному регламенту организации доступа к объектам информационной инфраструктуры

БЛОК-СХЕМА
процесса изменения доступа к объектам информационной инфраструктуры

Шаг	Исполнитель	Результат
1	ОК (инициатор договора)	Поставлена задача для прекращения доступа субъекта к объектам ИИ ОЗ. Представлена копия приказа или заполненная заявка на прекращение доступа.
2.1	Руководитель структурного подразделения (инициатор договора)	Определена необходимость сохранения доступа к учетным записям субъекта, его почтовому ящику и т.п. При отсутствии такой необходимости задача исполнена.
2.2		Внесены соответствующие сведения в заявку на прекращение доступа при необходимости сохранения доступа к учетным записям субъекта, его почтовому ящику и т.п. Заполненная заявка прикреплена в качестве результата исполнения задачи.
3.1	ОИБ	Согласовано прекращение доступа субъекту к объектам ИИ ОЗ. Соисполнителю (ОИТ) поставлена подзадача прекращения доступа субъекту к объектам ИИ ОЗ. Срок исполнения подзадачи не должен превышать дату последнего рабочего дня субъекта. Изъяты служебные СНИ (при наличии), выполнено их форматирование. Проведено информирование субъекта по вопросам ЗИ, распространение и (или) предоставление которой ограничено (собственником которой является ОЗ).
	Руководитель структурного	Служебный СНИ, изъятый у субъекта, проанализирован на предмет наличия ценной информации. Информация передана ОИБ.

Шаг	Исполнитель	Результат
	подразделения (инициатор договора)	
3.2	ОИБ	Согласовано сохранение доступа к учетным записям субъекта, его почтовому ящику и т.п. Соисполнителю (ОИТ) поставлена подзадача отмены доступа субъекту к объектам ИИ ОЗ. Срок исполнения подзадачи – не позднее даты, установленной заявкой. Изъяты служебные СНИ (при наличии), выполнено их форматирование. Проведено информирование субъекта по вопросам ЗИ, распространение и (или) предоставление которой ограничено (собственником которой является ОЗ).
	Руководитель структурного подразделения (инициатор договора)	Служебный СНИ, изъятый у субъекта, проанализирован на предмет наличия ценной информации. Информация передана ОИБ.
4.1	ОИТ	Согласовано прекращение доступа субъекту к объектам ИИ ОЗ. Учетная запись субъекта отключена на срок до 30 дней. Изменена конфигурация ресурсов и прав доступа. Определена необходимость прекращения доступа к информационным ресурсам и сервисам ОЗ не своей зоны ответственности.
4.2		Соисполнителю (администратору ресурса) поставлена подзадача прекращения доступа субъекту к информационным ресурсам и сервисам ОЗ. Срок исполнения подзадачи не должен превышать дату последнего рабочего дня субъекта.
4.3	Администратор ресурса	Отменен доступ к информационным ресурсам и сервисам своей зоны ответственности.
4.4	ОИТ	Согласовано сохранение доступа к учетным записям субъекта, его почтовому ящику и т.п. Определена необходимость прекращения доступа к информационным ресурсам и сервисам ОЗ не своей зоны ответственности.

Шаг	Исполнитель	Результат
		Учетная запись субъекта удалена не позднее даты, установленной заявкой. Изменена конфигурация ресурсов и прав доступа не позднее даты, установленной заявкой.
4.5	ОИТ	Соисполнителю (администратору ресурса) поставлена подзадача прекращения доступа субъекту к информационным ресурсам и сервисам ОЗ. Срок исполнения подзадачи – не позднее даты, установленной заявкой.
4.6	Администратор ресурса	Отменен доступ к информационным ресурсам и сервисам своей зоны ответственности не позднее даты, установленной заявкой.

Приложение 3
к Примерному регламенту организации доступа к объектам информационной инфраструктуры

БЛОК-СХЕМА
процесса изменения доступа к объектам информационной инфраструктуры

Шаг	Исполнитель	Результат
1	ОК	Поставлена задача изменения прав доступа субъекта к объектам ИИ ОЗ. Представлена копия приказа или извещение о соответствующем кадровом событии.
2.1	Руководитель структурного подразделения	Определена необходимость предоставления дополнительных прав доступа субъекта к объектам ИИ ОЗ. При отсутствии такой необходимости задача выполнена.
2.2		Внесены соответствующие сведения в заявку на предоставление доступа.
3.1	ОИБ	Согласовано изменение учетной записи субъекта и прав доступа к объектам ИИ ОЗ. Соисполнителю (ОИТ) поставлена подзадача изменения доступа субъекту к объектам ИИ ОЗ. Срок исполнения подзадачи – не позднее даты, установленной приказом. Проведено информирование переводимого работника по вопросам ЗИ, распространение и (или) предоставление которой ограничено (собственником которой является ОЗ).

Шаг	Исполнитель	Результат
4.1	ОИТ	Отключена локальная учетная запись субъекта для конкретного ресурса (при необходимости). Изменена конфигурация ресурсов и прав доступа не позднее даты, установленной приказом. Субъект проинформирован о предоставленных правах доступа. Определена необходимость изменения прав доступа субъекта к информационным ресурсам и сервисам ОЗ не своей зоны ответственности.
4.2		Соисполнителю (администратору ресурса) поставлена подзадача изменения прав доступа субъекту к объектам ИИ ОЗ (к корпоративным и (или) проектным информационным ресурсам и сервисам ОЗ).
4.3	Администратор ресурса	Отключена локальная учетная запись субъекта для конкретного ресурса (при необходимости). Изменены права доступа к информационным ресурсам и сервисам своей зоны ответственности.

Приложение 4
к Примерному регламенту организации доступа к объектам информационной инфраструктуры

БЛОК-СХЕМА
процесса изменения доступа к объектам информационной инфраструктуры по решению ОИБ и (или) ОИТ

Шаг	Исполнитель	Результат
1	ОИБ ОИТ Администратор ресурса	Учетная запись субъекта отключена, конфигурация ресурсов и прав доступа изменена на время проведения мероприятий по устранению и расследованию инцидента ИБ.
2	ОИБ ОИТ	Проанализированы журналы аудита. Опрошены лица, затронутые инцидентом ИБ. Проанализированы сведения об уязвимостях, с использованием которых были реализованы угрозы ИБ и которые привели к возникновению инцидента ИБ. Проанализированы данные, зафиксированные средствами ЗИ. Проанализированы действия по устранению инцидента ИБ. Установлены лица, действия или бездействие которых вызвали инцидент ИБ, и факт нарушения ими своих трудовых или договорных обязанностей.
3	Руководитель ОЗ	Принято решение о привлечении к ответственности работников ОЗ за нарушение требований по обеспечению ИБ.

4	ОИБ ОИТ Администратор ресурса	Учетная запись субъекта разблокирована, изменена конфигурация ресурсов и прав доступа.

Приложение 5
к Примерному регламенту организации доступа к объектам информационной инфраструктуры

Форма

ЗАЯВКА
на предоставление доступа

Фамилия, собственное имя, отчество (если таковое имеется)	
Структурное подразделение	
Должность	
Дата трудоустройства[1]	
Мобильный телефон[1]	
Дата рождения[1]	
Заполняется при заключении договора с подрядчиком:	
Дата заключения договора	
Сроки выполнения работы (оказания услуг)	
Фамилия, собственное имя, отчество (если таковое имеется) ответственного лица, который курирует деятельность подрядчика	
Должность ответственного лица, который курирует деятельность подрядчика	

Дополнительные права доступа[2]:

		Примечание
Разрешить подключение съемного носителя информации	☐	
Разрешить удаленный доступ к следующим ресурсам:		
система электронного документооборота	☐	
	☐	

[1] Обязательно для заполнения при первоначальном предоставлении доступа (в рамках трудоустройства).

[2] В случае, если форма заявки не содержит ресурсы, к которым необходимо получить дополнительные права доступа, лицо, формирующее заявку, вносит их самостоятельно.

Разрешить доступ к следующим информационным ресурсам и сервисам:		
	☐	
	☐	

Прошу установить следующее дополнительное программное обеспечение, не входящее в состав типового рабочего места[3]:

1

2

Должность *подпись* И.О.Фамилия

«число» месяц год

[3] При заполнении необходимо указать полное наименование запрашиваемого программного обеспечения, вид лицензионного соглашения (лицензионное, свободное).

Приложение 6
к Примерному регламенту организации доступа к объектам информационной инфраструктуры

Форма

ЗАЯВКА
на прекращение доступа

Фамилия, собственное имя, отчество (если таковое имеется)			
Структурное подразделение			
Должность			
Дата наступления кадрового события		Телефон	

Прошу сохранить доступ к _____
наименование учетной записи,

_____
почтового ящика, ресурсов и т.п.

на срок до _____
период времени

в связи с _____.
обоснование с указанием обоснованной причины

Должность *подпись* И.О.Фамилия

«число» месяц год

Приложение 7
к Примерному регламенту организации доступа к объектам информационной инфраструктуры

Форма

ИЗВЕЩЕНИЕ
о переводе (назначении на должность, перемещении)

Извещаем о предстоящем _____
переводе работника в другое

_____
структурное подразделение / назначении на новую должность / переводе на другую

_____
работу для замещения временно отсутствующего работника

Фамилия, собственное имя, отчество (если таковое имеется)			
Текущее структурное подразделение		Новое структурное подразделение	
Текущая должность		Новая должность	
		Замещаемая должность	
Дата наступления кадрового события		Телефон	

Должность *подпись* И.О.Фамилия

«число» месяц год