



ЗАГАД

19.03 2024 № 195

г.Мінск

ПРИКАЗ

г.Минск

Об утверждении Политики информационной безопасности

Во исполнение Закона Республики Беларусь от 10 ноября 2008 г. № 2 455-З «Об информации, информатизации и защите информации», других нормативно-правовых актов в отношении информационной безопасности и в связи с необходимостью совершенствования деятельности, направленной на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации

ПРИКАЗЫВАЮ:

1. Утвердить Политику информационной безопасности открытого акционерного общества «Минский завод гражданской авиации № 407» (далее – Политика).

2. Начальнику отдела информационных технологий обеспечить:

2.1. Размещение настоящей Политики в глобальной компьютерной сети Интернет на официальном сайте ОАО «Минский завод гражданской авиации № 407».

3. Руководителям структурных подразделений довести Политику, размещенную на Avia407 (P:)/Обмен данными/ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, до сведения подчиненных работников под роспись с представлением копий листов ознакомления в адрес отдела информационных технологий.

4. Контроль за исполнением настоящего приказа возложить на первого заместителя генерального директора Мацкалова А.А.

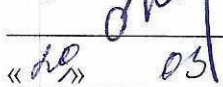
Генеральный директор

В.В.Пекарский

**Открытое акционерное общество
«Минский завод гражданской авиации № 407»**

СОГЛАСОВАНО

Первый ЗГД

 А.А. Мацкалов
«29» 03 2024г.

УТВЕРЖДЕНО

Приказ генерального директора
ОАО «Минский завод гражданской
авиации № 407»

29.03.2024 № 195

ПОЛИТИКА

информационной безопасности

ОАО «Минский завод гражданской авиации № 407»

**ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ**

1. **Политика информационной безопасности** (далее – Политика) открытого акционерного общества «Минский завод гражданской авиации № 407» (далее – Завод) разработана в соответствии с требованиями Положения о порядке технической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено, утвержденного приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66.

Нормативной правовой основой Политики служат:

Гражданский кодекс Республики Беларусь;

Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

Закон Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных»;

Указ Президента Республики Беларусь от 9 декабря 2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации»;

Постановление Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О концепции информационной безопасности Республики Беларусь»;

Приказ 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»;

иные нормативные правовые акты Республики Беларусь в области информатизации, безопасности и защиты информации, международные стандарты в области информационной безопасности продуктов и систем информационных технологий.

2. Политика определяет общие цели и принципы деятельности по защите Завода от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на **информационные системы (далее – ИС)**, а также минимизации рисков **информационной безопасности (далее – ИБ)**.

3. Настоящий документ не охватывает вопросы защиты информации, отнесенной к государственным секретам. Защита данного вида информации регламентируется соответствующими нормативными правовыми актами.

4. Положения Политики доводятся до ознакомления и являются обязательными для всех работников Завода, организующих и обеспечивающих эксплуатацию ИС при выполнении своих служебных обязанностей, иных пользователей ИС, физических или юридических лиц, выступающих в качестве информационных посредников, операторов информационных систем и связи.

5. Политика должна актуализироваться в связи с изменением законодательства Республики Беларусь в области защиты информации, изменениями в организационной структуре или в информационной инфраструктуре Завода. Поддержание положений Политики в актуальном состоянии осуществляет отдел информационных технологий (далее – ОИТ).

ГЛАВА 2

ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

6. Для целей Политики применяются термины в значениях, определенных в Указе Президента Республики Беларусь от 16 апреля 2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации», Законе Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации» (за исключением термина «персональные данные»), Законе Республики Беларусь от 7 мая 2021 г. № 99-З «О защите персональных данных», а также следующие термины и их определения:

администрирование ИС – предоставление пользователям соответствующих прав использования возможностей работы с ИС и обеспечение целостности данных;

активы – информация или ресурсы, которые должны быть защищены средствами системы защиты информации, используемыми в ИС;

анализ риска – систематическое использование информации для

выявления источников и оценки степени риска;

атака — попытка нарушения ИБ или попытка обхода средств управления безопасностью ИС;

аутентификация — проверка принадлежности субъекту доступа предъявленного им идентификатора, подтверждение подлинности;

доступность — свойство активов ИС, заключающееся в возможности их использования по требованию субъекта, имеющего соответствующие полномочия, за приемлемое время;

информационная безопасность — состояние защищенности информации и бизнес-процессов Завода, объединяющих в своем составе работников Завода, от внешних и внутренних угроз в информационной сфере;

информационная система — совокупность банков данных, информационных технологий и комплекса программно-технических средств (далее — КПТС), применяемых для обеспечения бизнес-процессов Завода;

инцидент информационной безопасности — одно или ряд нежелательных или непредвиденных событий в области ИБ, при которых имеется значительная вероятность компрометации функционирования деловых процессов или реализации угрозы ИБ;

комплекс программно-технических средств — совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий;

контролируемая зона — территория вокруг объекта информатизации, здание, часть здания, в пределах которого исключено неконтролируемое пребывание посторонних лиц и транспортных средств, не имеющих разрешения на постоянный или разовый доступ на объект;

конфиденциальность — свойство информации, обрабатываемой ИС, быть недоступной и закрытой от раскрытия и использования пользователями, лицами, логическими объектами или процессами ИС, которые не имеют соответствующих полномочий;

критический ресурс — объекты информационной сети, несанкционированный доступ к которым может повлечь за собой доступность информационных систем;

пользователь ИС — физическое лицо, обладающее правом доступа к ИС;

риск ИБ — потенциальная возможность реализации угроз ИБ, которая может повлечь нарушение или прекращение функционирования ИС;

система защиты информации (далее — СЗИ) — комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности

информации в ИС Завода;

событие ИБ – идентифицированное возникновение состояния ИС, услуги или сети, указывающее на возможное нарушение ИБ или отказ средств защиты, а также возникновение ранее неизвестной ситуации, которая может быть связана с безопасностью;

целостность – свойство сохранения полноты состава и неизменности активов ИС;

угроза – описание возможности воздействия на ИС в понятиях источник угроз (нарушитель), атака и актив, который подвергается атаке.

ГЛАВА 3

ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ

7. Целями защиты информации является защита Завода от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС, а также минимизация рисков ИБ.

8. Основными задачами Завода в части обеспечения безопасности информации в ИС являются:

- реализация требований законодательства Республики Беларусь в части информационной безопасности ИС и мер контроля их защищенности;

- определение ответственности субъектов информационных отношений по обеспечению и соблюдению требований Политики, в том числе с использованием программных, программно-аппаратных средств технической и криптографической защиты информации, а также посредством принятия соответствующих внутренних нормативных и организационно-методических документов информационной безопасности Завода;

- минимизация ущерба, который может быть нанесен Заводу из-за нарушений ИБ;

- разграничение доступа пользователей к ИС (предоставление доступа пользователям только к тем информационным ресурсам и выполнению только тех операций в ИС, которые необходимы пользователям для выполнения своих служебных обязанностей);

- обеспечение аутентификации пользователей;

- обеспечение регистрации действий пользователей ИС в системных журналах и организация контроля этих действий путем анализа содержимого журналов;

- обеспечение защиты от несанкционированной модификации используемого в ИС программного обеспечения (далее – ПО), а также защиты ИС от внедрения несанкционированных программ, включая вредоносное ПО;

обеспечение резервирования и архивирования информационных ресурсов;

обеспечение криптографической защиты информации, распространение и (или) предоставление которой ограничено, не отнесенной к государственным секретам, при ее передаче посредством сетей электросвязи общего пользования;

своевременное выявление и оценка причин, условий и характера угроз ИБ, дальнейшее прогнозирование и профилактика развития событий ИБ на основе мониторинга инцидентов ИБ;

выявление, предупреждение и пресечение возможности противоправной и иной деятельности работников Завода;

планирование, реализация и контроль эффективности использования защитных мер и СЗИ, создание механизма оперативного реагирования на угрозы ИБ;

реализация программ по осведомленности и обучению работников Завода о возможных факторах рисков ИБ и мерах противодействия.

ГЛАВА 4

СУБЪЕКТЫ И ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ПОРЯДОК ИХ ИНФОРМАЦИОННОГО ВЗАИМОДЕЙСТВИЯ

9. Субъектами информационной безопасности являются:

ответственные за ИБ в ИС – должностные лица Завода или структурные подразделения, обеспечивающие ИБ в те или иные ИС, определенные в пункте 34 настоящей Политики;

ответственное подразделение по защите сетевой и вычислительной инфраструктуры Завода – структурное подразделение, организующее разработку, внедрение и функционирование технической системы ИБ, имеющее в составе специалистов, выполняющих функции администратора ИБ ИС. Ответственным подразделением по информационной безопасности Завода является ОИТ;

пользователи ИС – работники Завода, использующие ИС для решения задач, возникающих в процессе выполнения должностных обязанностей на Заводе.

10. При планировании и реализации мероприятий по обеспечению ИБ на Заводе осуществляются:

инвентаризация информационных ресурсов Завода и уточнение состава ИС;

оценка важности (категорирование) информационных ресурсов и элементов ИС;

формирование методики оценки рисков (установление критериев

рисков для ИС и информационных ресурсов Завода и формирование методики обработки рисков);

проектирование, внедрение и поддержание в актуальном состоянии СЗИ;

разработка и поддержание в актуальном состоянии локальных правовых актов Завода по вопросам ИБ;

обучение пользователей ИС по вопросам ИБ.

11. Для проверки соответствия системы управления ИБ требованиям законодательства о защите информации, оценки степени (качества) защиты Завода от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС проводятся периодические аудиты ИБ согласно документации системы защиты информации.

12. В процессе эксплуатации ИС осуществляются:

контроль за соблюдением требований, установленных локальными правовыми актами Завода в области ИБ;

контроль за порядком использования ИС;

мониторинг функционирования ИС и СЗИ;

выявление угроз (анализ журналов аудита), которые могут привести к сбоям, нарушению функционирования ИС;

резервное копирование информации, содержащейся в ИС;

выявление и фиксация инцидентов ИБ, принятие мер по своевременному реагированию на инциденты ИБ, выполнению мероприятий по недопущению инцидентов ИБ.

13. На основе анализа функционирования системы управления ИБ в ходе эксплуатации ИС осуществляется постоянная оценка соответствия уровня защищенности ИС установленным критериям риска.

В случае несоответствия заданным критериям или их изменения производится корректировка СЗИ ИС.

14. Объектами ИБ являются:

информация, хранящаяся и обрабатываемая в ИС Завода, а также передаваемая на Завод (классификация информации, хранящейся и обрабатываемой в ИС Завода, представлена в разделе Перечень информационных систем);

КПТС, включающий технические, программные и программноаппаратные средства обработки, передачи и отображения информации, в том числе каналы передачи данных и информационного обмена, средства технической и криптографической защиты информации.

15. Основными составляющими КПТС Завода являются компоненты, входящие в состав корпоративной информационной

сети Завода:

- коммуникационная инфраструктура;
- информационные системы;
- программное обеспечение;
- автоматизированные рабочие места работников Завода.

16. КППТС должен располагаться в помещениях, исключающих несанкционированный доступ к ним и обеспечивающих их бесперебойную круглосуточную эксплуатацию в климатических условиях, указанных в документации на эксплуатацию.

17. Порядок информационного взаимодействия субъектов с объектами информационной безопасности Завода определяется локальными правовыми актами Завода.

18. Порядок информационного взаимодействия объектов между собой определяется эксплуатационной (технической) документацией на ИС Завода.

ГЛАВА 5

ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

19. ИБ Завода базируется на принципах конфиденциальности, целостности, подлинности, доступности и сохранности информации в ИС Завода.

20. Необходимый уровень безопасности достигается путем реализации мер, направленных на минимизацию возможного ущерба за счет:

- профилактики нарушения ИБ;
- своевременного обнаружения нарушений ИБ;
- эффективного восстановления нормального состояния ресурсов и функционирования ИС.

21. Обеспечение целостности и конфиденциальности информации и информационных ресурсов ИС достигается:

- управлением доступом пользователей к информации;
- резервным копированием информации и резервированием инфраструктуры;

- контролем действий пользователей, в частности действий, производимых с критическими ресурсами, влияющими на работоспособность ИС;

- наличием антивирусной защиты в составе СЗИ;
- средствами криптографической защиты информации (при необходимости).

22. Доступность информационных ресурсов и услуг ИС пользователям обеспечивается:

- резервированием аппаратных и программных средств ИС;

наличием регулярно актуализируемых и проверенных на практике планов обеспечения непрерывной работы и восстановления ИС;

наличием соглашения с оператором сети Интернет об уровне предоставления сервиса, содержащим описание услуги, права и обязанности сторон, согласованный уровень качества предоставления услуги (доступность, надежность, безопасность и управляемость);

наличием документированных процедур, регламентирующих процессы жизненного цикла программно-технических средств, направленных на обеспечение непрерывности функционирования ИС.

23. Подлинность пользователя ИС достигается за счет средств аутентификации ИС.

24. Сохранность информационных ресурсов и услуг ИС достигается за счет системы хранения данных и реализации резервного копирования.

25. Управление инцидентами ИБ осуществляется в соответствии с установленными правилами управления инцидентами ИБ в ИС.

26. Для всех критических ресурсов определяются правила, установленные локальными правовыми актами.

27. Порядок и правила предоставления доступа к объектам информационной безопасности Завода определяется локальными правовыми актами Завода.

28. Работникам Завода предоставляется уровень доступа к объектам ИБ Завода в объеме, необходимом для выполнения своих должностных обязанностей.

29. Физический доступ к КПТС (охраняемые зоны, периметры безопасности и т.п.) обеспечивается в соответствии с локальными правовыми актами.

Технические средства защиты оборудования должны включать в себя источники бесперебойного питания, трансформаторы и кондиционеры.

30. Работы в серверных помещениях должны производиться по согласованию с ответственным подразделением по ИБ и под контролем ответственного лица по структурному подразделению.

31. Размещение ИС, обрабатывающих информацию ограниченного распространения, в виртуальной инфраструктуре центров обработки данных сторонних организаций, предоставляющих соответствующие услуги, должно производиться исключительно при условии выполнения данными организациями требований законодательства Республики Беларусь в сфере защиты информации и по согласованию с ОИТ.

ГЛАВА 6

ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИС

32. Пользователи ИС должны:

осуществлять любые действия в ИС, к которым предоставлен доступ, после авторизации с использованием персональной учетной записи, зарегистрированной в ИС Завода;

использовать персональные компьютеры исключительно для тех целей, для которых они были предоставлены;

использовать в своей деятельности легально приобретенное ПО;

использовать доступные механизмы ИБ для защиты конфиденциальности и целостности собственной информации, когда это требуется;

устанавливать и использовать пароли в соответствии с требованиями локальных правовых актов по вопросам ИБ;

немедленно уведомлять ответственное лицо по структурному подразделению или ответственное подразделение за ИБ о возможной компрометации паролей авторизованного доступа к ИС;

блокировать доступ к ИС при уходе с рабочего места для предотвращения использования ИС неавторизованными пользователями.

33. Любое использование оборудования для целей, не связанных со служебной деятельностью, расценивается как несанкционированное использование оборудования.

Несанкционированная деятельность субъектов ИБ может обнаруживаться любыми незапрещенными законодательством способами и должна незамедлительно пресекаться.

ГЛАВА 7

ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ

34. На Заводе функционируют следующие ИС:

программный продукт «1С: Предприятие. Бухгалтерия 8»;

официальный интернет-сайт www.407@avia407.by;

система электронного документооборота «Directum».

35. Для обеспечения работоспособности ИС используются системы виртуализации Microsoft и VMWare, OpenStack, структурированная кабельная система, сервера с операционной системой семейства Windows и семейства Linux. Для доступа к информационным системам используются персональные компьютеры, находящиеся во внутренней сети Завода с операционными системами семейства Windows и семейства Linux.

36. При увольнении работника предоставленные пользователю права

доступа к системе электронного документооборота «Directum» удаляются. При увольнении работника руководитель структурного подразделения уведомляет ОИТ с помощью докладной записки о лишении прав доступа работника Завода к системе электронного документооборота «Directum», программному продукту «1С: Предприятие. Бухгалтерия 8».

ГЛАВА 8

ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

37. Порядок взаимодействия объектов ИБ Завода с ИС Завода определяется локальными документами по каждому взаимодействию.

38. Обновление баз средств антивирусной защиты информации должно осуществляться с периодичностью, рекомендованной производителем антивирусного программного обеспечения.

39. Правила доступа к локальной вычислительной сети регулируются приказом генерального директора.

40. Синхронизация времени программных средств коммутационного оборудования, компьютеров, серверов, центра обработки данных (далее – объектов Завода) осуществляется ежедневно в автоматическом режиме.

41. Функционирование объектов Завода должно осуществляться с синхронизацией времени с Интернет-ресурсом Белорусского государственного института метрологии belgim.by и обновлением системного, прикладного программного обеспечения и антивирусных баз с соответствующими ресурсами.

42. К авторизованным сервисам Завода относятся:

обновление системного и прикладного ПО;

обновление встроенного ПО технических средств;

обновление антивирусных средств защиты информации;

синхронизация времени с источником надежного времени.

43. Взаимодействие объектов Завода с иными ИС определяются соответствующими документами. Для взаимодействия объектов Завода с иными ИС должны применяться СЗИ, имеющие сертификат соответствия, выданный в Национальной системе подтверждения соответствия Республики Беларусь, или положительное экспертное заключение по результатам государственной экспертизы при Оперативно-аналитическом центре при Президенте Республики Беларусь.

ГЛАВА 9

ПОРЯДОК ОРГАНИЗАЦИИ ДИСТАНЦИОННОЙ РАБОТЫ

44. Работникам Завода (при необходимости) предоставляется автоматический доступ для дистанционной работы при помощи технологии VPN.

45. Для организации дистанционной работы при помощи технологии VPN руководители (начальники) структурных подразделений формируют списки работников, ИС и ресурсов (сервисов) Завода с обоснованием необходимости дистанционной работы.

46. Организацию и согласование удаленного доступа при помощи технологии VPN к ИС Завода осуществляет ОИТ. Если есть возможность рисков ИБ Завода, то ОИТ вправе отказать в удаленном доступе к ИС Завода.

47. Для обеспечения дистанционной работы при помощи технологии VPN с ИС Завода и ресурсами (сервисами) Завода, ОИТ вправе создавать дополнительные средства (методы) аутентификации работников Завода.

И.о.начальника отдела
информационных технологий



подпись

Д.В. Корзун