Открытое акционерное
общество «БЕЛЛИС»
(ОАО «БЕЛЛИС»)

Приложение 2

УТВЕРЖДЕНО
приказом №160
от «28» 11 2025

ПОЛИТИКА
ОАО «БЕЛЛИС» в отношении
информационной и кибербезопасности

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности и кибербезопасности (далее – Политика) ОАО «БЕЛЛИС» 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»;

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

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

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах 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

ОАО «БЕЛЛИС» от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на информационные системы (далее – ИС), а также минимизации рисков информационной и кибербезопасности (далее – ИБ и КБ).

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 работников ОАО «БЕЛЛИС», организующих или обеспечивающих эксплуатацию ИС при выполнении своих служебных обязанностей.

5. Политика должна актуализироваться в связи с изменением в законодательстве Республики Беларусь в области защиты информации, изменениями в организационной структуре или в информационной инфраструктуре ОАО «БЕЛЛИС».

ГЛАВА 2
ОСНОВНЫЕ ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

6. Для целей Политики применяются термины в значениях, определенных в Положении о технической и криптографической защите 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 – это 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 ОАО «БЕЛЛИС» 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 ОАО «БЕЛЛИС»;

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 ОАО «БЕЛЛИС»;

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;

кибербезопасность (далее – КБ) — это комплекс мер для защиты сетей,

устройств, программ и данных от цифровых угроз и кибератак, таких как кража, изменение или уничтожение информации.

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

ГЛАВА 3
ЦЕЛИ И ЗАДАЧИ ЗАЩИТЫ ИНФОРМАЦИИ И КИБЕРБЕЗОПАСНОСТИ

7. Целями защиты информации (кибербезопасности) является защита ОАО «БЕЛЛИС» от возможного нанесения материального, физического или иного ущерба посредством случайного или преднамеренного воздействия на ИС, а также минимизация рисков ИБ.

8. Основными задачами ОАО «БЕЛЛИС» 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 ОАО «БЕЛЛИС»;

минимизация ущерба, который может быть нанесен ОАО «БЕЛЛИС» 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 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;

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

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

реализация программ по осведомленности работников 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, обеспечивающие ИБ в той или иной ИС, корректное и безопасное функционирование ИС, компьютеров и сети;

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

10. В процессе эксплуатации ИС осуществляются:

контроль за соблюдением требований, установленных локальными правовыми актами ОАО «БЕЛЛИС» 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 (киберугроз), принятие мер по своевременному реагированию на инциденты ИБ, выполнению мероприятий по недопущению инцидентов ИБ.

11. 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.

12. Объектами ИБ являются:

информация, хранящаяся и обрабатываемая в ИС ОАО «БЕЛЛИС», а также передаваемая в ОАО «БЕЛЛИС» при оказании услуг (классификация информации, хранящейся и обрабатываемой в ИС;

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

13. Основными составляющими КПТС являются компоненты, входящие в состав корпоративной информационной сети ОАО «БЕЛЛИС»:

коммуникационная инфраструктура;

информационные системы;

программное обеспечение;

автоматизированные рабочие места работников.

14. КПТС должен располагаться в помещениях, исключающих

несанкционированный доступ к ним и обеспечивающих их бесперебойную круглосуточную эксплуатацию в климатических условиях, указанных в документации на эксплуатацию.

15. Порядок информационного взаимодействия субъектов с объектами информационной безопасности ОАО «БЕЛЛИС» определяется локальными правовыми актами ОАО «БЕЛЛИС».

ГЛАВА 5
ОСНОВНЫЕ ПРИНЦИПЫ ЗАЩИТЫ ИНФОРМАЦИИ

16. ИБ ОАО «БЕЛЛИС» базируется на принципах конфиденциальности, целостности, подлинности, доступности и сохранности информации в ИС.

17. 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.

18. 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).

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

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

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

22. Для всех критических ресурсов определяются правила, установленные Положением о копировании, резервировании и восстановлении информации.

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

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

ГЛАВА 6
ОБЯЗАННОСТИ ПОЛЬЗОВАТЕЛЕЙ ИС

24. Пользователи ИС должны:

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

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 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.

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

ГЛАВА 7
ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ СИСТЕМ

25. В ОАО «БЕЛЛИС» функционируют следующие ИС:

электронный почтовый сервис;

автоматизированная ИС «1С Бухгалтерия»;

ИС «SMBusiness»;

система видеоконференцсвязи;

сайт ОАО «БЕЛЛИС»;

система контроля доступа;

система видеонаблюдения.

26. Для обеспечения работоспособности ИС используются системы виртуализации Microsoft Hyper-V и VMWare ESXi, OpenStack, структурированная кабельная система, сервера с операционной системой семейства Windows и семейства Linux. Для доступа к информационным

системам используются персональные компьютеры.

27. Электронный почтовый сервис, доступный по адресу ms1.g-cloud.by с доменным именем bellis.by, относится к классу 3-юл. Администрирование обеспечивает администратор сетей.

28. Администрирование автоматизированной ИС «Контроль доступа» обеспечивает обслуживающая организация. Доступ к редактированию информации, автоматизированной ИС «Контроль доступа» предоставляется пользователям ИС, которым в рамках выполнения должностных обязанностей необходима информация, содержащаяся в данной ИС либо согласно приказу директора.

Права, предоставляемые пользователю ИС, определяются секретарем приемной комиссии. Доступ к личному кабинету абитуриента, который является частью ИС «Абитуриент», получают пользователи, зарегистрировавшиеся на данном ресурсе. Информационную безопасность данной ИС осуществляет ЦИТ.

29. Администрирование и эксплуатацию Автоматизированная ИС «1 С Бухгалтерия» осуществляет ПФО-бухгалтерия. Доступ к автоматизированной ИС «1 С Бухгалтерия» получают пользователи, которым в рамках выполнения должностной обязанностей необходима информация, содержащаяся в данной ИС. ИБ данной ИС осуществляет ПФО-бухгалтерия, администратор сетей, и/или разработчики, и/или обслуживающая организация при технической поддержке администратора сетей в части безопасности на сетевом уровне.

30. ИС «SMBusiness» относится к классу 2-ПДн. Администрирование ИС осуществляется администратором сетей, секретарем приемной руководителя. Доступ к ИС «SMBusiness» работники ОАО «БЕЛЛИС» осуществляют в соответствии с приказом директора. Информационную безопасность данной ИС осуществляют секретарь приемной руководителя, администратор сетей, и/или разработчики, и/или обслуживающая организация.

31. Система видеоконференцсвязи относится к классу 3-ин. Администрирование ИС обеспечивает администратор сетей.

32. Сайт ОАО «БЕЛЛИС», доступен по адресу www.bellis.by. Администрирование обеспечивает администратор сетей. Право на редактирование сайта БГУ имеет администратор сетей. Информационную безопасность данной ИС осуществляет администратор сетей, и/или разработчики, и/или обслуживающая организация при технической поддержке администратора сетей.

33. Технические аспекты защиты сетевой и вычислительной инфраструктуры ОАО «БЕЛЛИС» возлагаются на администратора сетей.

34. При увольнении работника все предоставленные пользователю права

доступа к ресурсам ИС удаляются. При изменении трудовых отношений руководитель структурного подразделения уведомляет администратора сетей с помощью докладной записки о лишении прав доступа работника к ИС.

ГЛАВА 8
ПОРЯДОК ВЗАИМОДЕЙСТВИЯ С ИНЫМИ ИНФОРМАЦИОННЫМИ СИСТЕМАМИ

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

36. Синхронизация времени программных средств коммутационного оборудования, компьютеров, серверов осуществляется ежедневно в автоматическом режиме.

37. К авторизованным сервисам ОАО «БЕЛЛИС» относятся:

обновление системного и прикладного ПО;

обновление встроенного ПО технических средств;

обновление антивирусных средств защиты информации;

синхронизация времени с источником надежного времени.

Специалист по кадрам-юрисконсульт И.В. Миранович

Согласовано:

Специалист по организации закупок-юрисконсульт _____А.С.Король «28» 11 2025

Администратор сетей _____А.С.Крайник «28» 11 2025