Государственный комитет по стандартизации Республики Беларусь

Республиканское унитарное предприятие

«Белорусский государственный центр аккредитации»

**ПОЛОЖЕНИЕ**

**О ПОРЯДКЕ ОБЕСПЕЧЕНИЯ**

**ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

|  |  |
| --- | --- |
| Разработано | Сектором информационных технологий |
| Ответственный за пересмотр | Сектор информационных технологий |
| Утверждено | Приказом от 27.12.2024 №156 |
| Введено в действие | 03.01.2025 |
| Редакция | 05 |
| Изменение  |  |
| Экземпляр | Контрольный  |
| Взамен | Положения о порядке обеспечения информационной безопасности, редакция 04 |

СОДЕРЖАНИЕ

[**1 ОБЛАСТЬ ПРИМЕНЕНИЯ** 3](#_Toc187241414)

[**2 ССЫЛКИ** 3](#_Toc187241415)

[**3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ** 4](#_Toc187241416)

[**4 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ** 7](#_Toc187241417)

[**5 ОТВЕТСТВЕННОСТЬ И ПОЛНОМОЧИЯ** 7](#_Toc187241418)

[**6 ОСНОВНЫЕ ПОЛОЖЕНИЯ** 11](#_Toc187241419)

[**7 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИБ** 11](#_Toc187241420)

[**8 ОРГАНИЗАЦИЯ РАБОТЫ С ОИС ПРЕДПРИЯТИЯ** 13](#_Toc187241421)

[**9 ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ** 15](#_Toc187241422)

[**10 ОСНОВНЫЕ ОРГАНИЗАЦИОННЫЕ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО СОЗДАНИЮ И ОБЕСПЕЧЕНИЮ ФУНКЦИОНИРОВАНИЯ СЗИ** 15](#_Toc187241423)

[**11 ПОРЯДОК ПЕРЕСМОТРА ПОЛОЖЕНИЯ** 18](#_Toc187241424)

[**Приложение 1**](#_Toc187241425) [Инструкция об организации доступа в сеть Интернет 19](#_Toc187241426)

[**Приложение 2**](#_Toc187241427) [Инструкция об организации работы и использованию электронной почты 21](#_Toc187241428)

[**Приложение 3**](#_Toc187241429) [Порядок действий по устранению инцидентов ИБ 26](#_Toc187241430)

[**Приложение 4**](#_Toc187241431) [Перечень разрешенного для работы ПО 28](#_Toc187241432)

[**Приложение 5**](#_Toc187241433) [Краткая инвентаризационная опись активов предприятия 29](#_Toc187241434)

[**Приложение 6**](#_Toc187241435) [Организация доступа к ИС «Аккредитация» 31](#_Toc187241436)

[**Приложение 7**](#_Toc187241437) [Порядок работы с информационным ресурсе БГЦА (BSCA) 32](#_Toc187241438)

[**Приложение 8**](#_Toc187241439) [Инструкция по использованию парольной защиты 35](#_Toc187241440)

[**Приложение 9**](#_Toc187241441) [Порядок функционирования шлюза информационной безопасности (межсетевого экрана) 37](#_Toc187241442)

[**Приложение 10**](#_Toc187241443) [Организация доступа и резервного копирования информации 38](#_Toc187241444)

[**Приложение 11**](#_Toc187241445) [Регламент доступа к администрированию ОИС 39](#_Toc187241446)

# **1 ОБЛАСТЬ ПРИМЕНЕНИЯ**

**1.1** Настоящее положение является документом системы менеджмента Государственного предприятия «БГЦА», разработано в развитие п.7.14 ГОСТ ISO/IEC 17011, представляет собой совокупность необходимых требований в области защиты информации, регламентирующих информационное взаимодействие на предприятии, и предназначено для обеспечения информационной безопасности и организации использования сети Интернет и электронной почты на предприятии, в том числе для реализации требований отраслевых рекомендаций системы Госстандарта, требований Директивы Президента Республики Беларусь от 11 марта 2004 г. № 1 «О мерах по укреплению общественной безопасности и дисциплины».

**1.2** Требования настоящего положения обязательны для применения персоналом БГЦА.

# **2 ССЫЛКИ**

2.1 Правовую основу обеспечения ИБ БГЦА составляют положения следующих нормативных правовых актов:

Конституции Конституция Республики Беларусь;

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

Закон Республики Беларусь от 5 мая 1999 г. № 250-З «О научно-технической информации»;

Закон Республики Беларусь от 8 ноября 2018 г. № 143-З «Об электронном документе и электронной цифровой подписи»;

Кодекс Республики Беларусь об административных правонарушениях от 6 января 2021 г.
№ 91-З;

Процессуально-исполнительный Кодекс Республики Беларусь об административных правонарушениях от 6 января 2021 г. № 92-З;

Уголовный Кодекс Республики Беларусь от 9 июля 1999 г. № 275-З

Уголовно-исполнительный Кодекс Республики Беларусь от 11 января 2000 г. № 365-З;

Уголовно-процессуальный Кодекс Республики Беларусь от 16 июля 1999 г. № 295-З;

Указ Президента Республики Беларусь от 09.12.2019 №449 «О совершенствовании государственного регулирования в области защиты информации»;

Указ Президента Республики Беларусь от 01.02.2010 № 60 (ред. от 18.09.2019) «О мерах по совершенствованию использования национального сегмента сети Интернет»;

ОРГ 3.01 Отраслевые рекомендации по обеспечению информационной безопасности в организациях системы Госстандарта, утвержденными Приказом Председателя Государственного комитета по стандартизации Республики Беларусь от 03.09.2024 № 122;

ОРГ 3.02 «Отраслевые рекомендации по использованию сети Интернет и электронной почты в организациях системы Госстандарта», утвержденными Приказом Председателя Государственного комитета по стандартизации Республики Беларусь от 02.09.2024 № 121;

СТБ ISO/IEC 27000-2012 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь;

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

СТБ 34.101.8-2006 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Общие требования;

СТБ 34.101.9-2004 Информационные технологии. Требования к защите информации от несанкционированного доступа, устанавливаемые в техническом задании на создание автоматизированной системы;

СТБ 34.101.10-2004 Информационные технологии. Средства защиты информации от несанкционированного доступа в автоматизированных системах. Общие требования;

СТБ 34.101.11-2009 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты операционной системы сервера для использования в доверенной зоне корпоративной сети;

СТБ 34.101.12-2007 Информационные технологии. Методы и средства безопасности. Программные средства защиты от воздействия вредоносных программ и антивирусные программные средства. Оценка качества;

[СТБ 34.101.14-2017](http://ips/TnpaDetail.php?UrlId=511085) Информационные технологии. Методы и средства безопасности. Программные средства маршрутизатора. Общие требования;

СТБ 34.101.16-2009 Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Профиль защиты программных средств коммутатора для использования в доверенной зоне корпоративной сети;

СТБ 34.101.18-2009 Информационные технологии. Синтаксис обмена персональной информацией;

[СТБ 34.101.30-2017](http://ips/TnpaDetail.php?UrlId=501245) Информационные технологии. Методы и средства безопасности. Информационные системы. Классификация;

Рекомендации оперативно-аналитического центра при Президенте Республики Беларусь государственным органам и иным организациям (в том числе владельцам критически важных объектов информатизации) по выполнению обязательных для исполнения требований законодательства в сфере технической и криптографической защиты информации, обеспечения кибербезопасности;

ПЛ СМ 9.4.1 Политика по обеспечению информационной безопасности.

# **3 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ**

В настоящем положении применяют термины, установленные в Законе Республики Беларусь от 10 ноября 2008 года «Об информации, информатизации и защите информации», в Положении о технической и криптографической защите информации в РБ, утвержденном Указом Президента Республики Беларусь 16.04.2013 №196, в [СТБ ISO/IEC 27000-2012](https://ips3.belgiss.by/TnpaDetail.php?UrlId=381002) «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Основные положения и словарь», а также следующие термины с соответствующими определениями:

* 1. **информация**: Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
	2. **документированная информация**: Информация, зафиксированная на материальном носителе с реквизитами, позволяющими ее идентифицировать;
	3. **база данных**: Совокупность структурированной и взаимосвязанной информации, организованной по определенным правилам на материальных носителях;
	4. **доступ к информации**: доступ к информации – комплекс организационно-технических мероприятий, позволяющих сотруднику получить возможность ознакомления с информацией, в том числе с помощью технических средств, в соответствии с предоставленными ему для этого правами;
	5. **управление доступом**: Средство для обеспечения того, что доступ к активам осуществляется при условии авторизации и ограничивается на основе бизнес-требований и требований безопасности;
	6. **аутентичность**: Свойство, заключающееся в том, что логический объект соответствует заявленному о себе;
	7. **доступность**: Свойство нахождения в состоянии готовности и пригодности для использования по запросу авторизированного логического объекта;
	8. **конфиденциальность информации**: Требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами Республики Беларусь;
	9. **информационная безопасность**: Сохранение конфиденциальности, целостности и доступности информации, а также другие свойства, такие как аутентичность, подотчетность, неопровержимость;
	10. **защита информации**: Комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;
	11. **защита информации от несанкционированного воздействия**: Деятельность, направленная на предотвращение воздействия на защищаемую информацию с нарушением установленных прав, и(или) правил на изменение информации, приводящего к её искажению, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;
	12. **информационная безопасность**: Сохранение конфиденциальности, целостности и доступности информации, а также другие свойства, такие, как аутентичность, подотчетность, неопровержимость и безотказность;
	13. **безопасность информации**: Состояние информации, информационных ресурсов и информационных систем, при котором с требуемой вероятностью обеспечивается защита информации (данных) от утечки, хищения, утраты, несанкционированного уничтожения, искажения, модификации (подделки), копирования, блокирования информации и т.п.;
	14. **информационная технология**: Совокупность процессов, методов осуществления поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения и (или) предоставления информации, а также пользования информацией и защиты информации;
	15. **комплекс программно–технических средств**: Совокупность программных и технических средств, обеспечивающих осуществление информационных отношений с помощью информационных технологий;
	16. **информационные отношения**: Отношения, возникающие при поиске, получении, передаче, сборе, обработке, накоплении, хранении, распространении и (или) предоставлении информации, пользовании информацией, защите информации, а также при применении информационных технологий;
	17. **информационная система**: Совокупность банков данных, информационных технологий и комплекса (комплексов) программно-технических средств;
	18. **информационная система Предприятия**: совокупность средств вычислительной техники, сетевого оборудования, системного и прикладного программного обеспечения, средств защиты информации, объединенного в единую систему посредством локальной вычислительной сети и внешних каналов связи;
	19. **объекты информационной системы:** Средства вычислительной техники, сетевое оборудование, системное и прикладное программное обеспечение, средства защиты информации;
	20. **доступ к информационной системе**: Возможность использования информационной системы и (или) информационной сети;
	21. **информационный ресурс**: Организованная совокупность документированной информации, включающая базы данных, другие совокупности взаимосвязанной информации в информационных системах;
	22. **аутентификация**: Предоставление гарантии того, что заявленная характеристика логического объекта является правильной;
	23. **актив**: Всё, что имеет ценность для организации;

Примечание– Существуют различные типы активов, включая:

- информацию;

- программное обеспечение, такое как компьютерная программа;

- аппаратное обеспечение, такое как компьютер;

- услуги;

- людей и их квалификацию, навыки и опыт;

- нематериальные активы, такие как репутация и имидж.

В контексте данного Положения подразумеваются активы, непосредственно связанные с информационными технологиями.

* 1. **информационный актив**: Знания или данные, которые имеют ценность для организации;
	2. **инцидент**: Одно или ряд нежелательных или непредвиденных событий в области информационной безопасности, при которых имеется значительная вероятность компрометации функционирования бизнеса и угрозы информационной безопасности;
	3. **межсетевой экран**: Комплекс аппаратных, программных или программно-аппаратных средств, осуществляющий контроль и фильтрацию проходящих через него сетевых пакетов на различных уровнях сетевой модели в соответствии с заданными правилами;
	4. **несанкционированный доступ**: Противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа;
	5. **обработка информации:** Совокупность операций сбора, накопления, ввода, вывода, приёма, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией;
	6. **средства вычислительной техники**: Совокупность математических и технических средств, методов и приемов, которые используются для облегчения и ускорения решения трудоемких задач, связанных с обработкой информации (персональные компьютеры, мониторы, принтеры, сканеры, ноутбуки, серверы);
	7. **средства защиты информации:** Специальные технические средства, используемые для предупреждения несанкционированного использования всех видов информации.

По вариантам использования различаются средства защиты информации:

индивидуальные, применяемые только одним сотрудником для защиты информации, используемой им самим;

сетевые, применяемые для защиты в вычислительных сетях и сетях связи.

* 1. **угроза безопасности информации**: Совокупность условий и факторов, создающих потенциальную или реально существующую опасность, связанную с утечкой информации и/или несанкционированным и/или непреднамеренным воздействиям на неё;
	2. **утечка информации**: Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она доверена, по техническим каналам утечки информации;
	3. **локальная вычислительная сеть**: Совокупность средств вычислительной техники, находящихся на географически ограниченной территории (офиса, здания), соединенных линиями связи, образованными кабелями, сетевыми адаптерами и другим коммуникационным оборудованием;
	4. **программное обеспечение**: Компьютерные программы, процедуры и, возможно, соответствующая документация и данные, относящиеся к функционированию компьютерной системы;
	5. **обладатель информации**: Субъект информационных отношений, получивший права обладателя информации по основаниям, установленным актами законодательства РБ, или по договору;
	6. **криптографическая защита информации**: Деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты информации;
	7. **носитель ключевой информации**: Малогабаритное USB-устройство, предназначенное для защищенного хранения личных ключей пользователей (абонентов) программного средства криптографической защиты информации;
	8. **пользователи**: Персонал Государственного предприятия «БГЦА», получивший доступ к комплексам программно-технических средств, программному обеспечение, средствам вычислительной техники, информационным сетям, ресурсам и системам, в том числе средствам защиты информации предприятия и использующий их в рамках выполнения своих функциональных обязанностей;
	9. **интернет**: Всемирная система объединенных компьютерных сетей, построенная на использовании протокола Internet Protocol (IP) и маршрутизации пакетов данных. Интернет образует глобальное информационное пространство;
	10. **электронная почта**: Сервис обмена электронными сообщениями в сети Интернет;
	11. **электронный почтовый ящик**: Персональное пространство на почтовом сервере, в котором хранятся электронные сообщения;
	12. **электронное почтовое сообщение**: Сообщение, формируемое отправителем с помощью почтового клиента и предназначенное для передачи получателю посредством электронной почты
	13. **аутентификация**: Предоставление гарантии того, что заявленная характеристика логического объекта является правильной.

# **4 ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ**

В настоящем положении применяют следующие обозначения и сокращения:

|  |  |
| --- | --- |
| БГЦА, предприятие | – Республиканское унитарное предприятие «Белорусский государственный центр аккредитации»; |
| БДЗИИБИРИС ПредприятияИС «Аккредитация»ИТЛВСЛПАНКИНПАСИТСИТОС ПК ПОРБ СВТСЗИОИСОАЦ | – база данных;– защита информации;– информационная безопасность;– информационный ресурс;– информационная система БГЦА;– информационная система «Аккредитация»;– информационная технология;– локальная вычислительная сеть;– локальный правовой акт;– носитель ключевой информации;– нормативный правовой акт;– сектор информационных технологий;– операционная система;– персональные компьютеры (стационарные, ноутбуки);– программное обеспечение;– Республика Беларусь;– средства вычислительной техники;– средства защиты информации;– объекты информационной системы;– оперативно-аналитический центр при Президенте РБ. |

# **5 ОТВЕТСТВЕННОСТЬ И ПОЛНОМОЧИЯ**

**5.1** Права обладателя информации не распространяются на ИР, ИС и ОИС, принадлежащие собственнику, с помощью которых осуществляются поиск, получение, передача, сбор, обработка, накопление, хранение, распространение и (или) предоставление и пользование информацией.

**5.2** Все пользователи несут персональную ответственность за свои действия (либо – бездействие) и невыполнение требований данного положения. При несоблюдении пользователями положений к ним могут быть применены меры дисциплинарной, административной, уголовной ответственности в соответствии с правовыми актами РБ.

**5.3** Предприятие не несет ответственности за действия отдельных пользователей, нарушивших требования настоящего положения, и имеет право проверять любой или все аспекты ИБ, чтобы гарантировать соблюдение положения.

**5.4** Руководитель предприятия:

осуществляет общее руководство системой ИБ;

принимает все решения по вопросам функционирования системы ИБ;

осуществляет контроль за организацией работы по ИБ;

обеспечивает выделение соответствующих материальных и кадровых ресурсов для поддержки на должном уровне процесса обеспечения ИБ Предприятия;

отвечает за поддержку процесса обеспечения ИБ Предприятия.

**5.5** Заместитель директора по аккредитации Предприятия обеспечивает ИБ по направлениям в соответствии с распределением обязанностей.

 **5.6** Работники СИТ осуществляют:

создание системы защиты информации;

разработку, внедрение и совершенствование систем ИБ с учетом возможных материальных затрат, финансовых и кадровых ресурсов предприятия;

анализ рисков (угроз) в области ЗИ и принятие соответствующих мер для устранения или минимизации количества и степени влияния рисков ИБ на Предприятие;

анализ обнаруженных проблем в области ИБ с целью оценки ситуации и формирования предложений директору по предотвращению последствий нарушения безопасности и\или в целях исключения повторяемости проблем;

анализ событий инцидентов и принятие соответствующих мер для минимизации вероятности возникновения инцидентов ИБ и сокращения повторяемости инцидентов ИБ;

контроль за соблюдением всеми пользователями Предприятия без исключения требований ЛПА по обеспечению ИБ;

общий контроль за использованием сети Интернет и электронной почты;

организация резервного копирования критически важных объектов информационной инфраструктуры;

обеспечение централизованного сбора и хранения не менее одного года информации о состоянии средств защиты информации, сетевого оборудования, систем, сервисов (netflow-трафик, лог-файлы запросов пользователей к локальным системам доменных имен, лог-файлы системы проксирования подключения к сети Интернет, лог-файлы предоставления пользователям динамических ip-адресов, лог-файлы работы серверов и др.), о действиях пользователей, а также о событиях ИБ;

Работники несут ответственность за использование сети Интернет и электронной почты, обеспечение ИБ в информационных системах и ресурсах в рамках своих полномочий. Обязанности по обеспечению ИБ содержатся в положении и должностных инструкциях работников СИТ.

**5.7** Начальник СИТ:

контролирует проведение работ по ЗИ с использованием ОИС персоналом СИТ;

своевременно пересматривает и вносит изменения в ЛПА по обеспечению ИБ.

**5.8** Начальник ОПКР:

организует внесение соответствующих изменений в ЛПА Предприятия;

своевременно информирует СИТ об изменениях статуса каждого работника (переход в другое подразделение, увольнение, приём на работу и т.п.).

**5.9** Руководители структурных подразделений Предприятия имеют право на просмотр информации своих подчиненных в соответствии со своими должностными обязанностями.

Руководители структурных подразделений Предприятия обязаны:

обеспечить закрепление каждой рабочей станции в своих подразделениях за пользователем, отвечающим за его безопасность и имеющего достаточную квалификацию для выполнения этой роли. Исключение составляют ПК, использующиеся для проведения видеоконференцсвязи, обучения и тренингов. Использование указанных ПК контролирует начальник соответствующего подразделения, за которым закреплены указанные ПК;

обеспечить соблюдение работниками их структурного подразделения установленных требований настоящего положения, вносить требования по обеспечению ИБ в должностные инструкции своих подчиненных;

пресекать факты нарушения работниками их структурного подразделения требований данного положения ИБ.

**5.10** Пользователи предприятия обязаны:

соблюдать требования ЛПА по обеспечению ИБ;

сообщать работникам СИТ обо всех инцидентах и событиях, связанных с ИБ;

использовать доступные защитные механизмы для обеспечения конфиденциальности и целостности своей информации, находящейся на ПК либо в ИР и ИС (в частности – периодически выполнять архивирование и создавать резервные копии информации, во избежание потери созданной вами документированной информации);

выполнять перезагрузку ПК по требованию системы после ее автоматического обновления;

оказывать посильную помощь другим пользователям в соблюдении ИБ, указывать им на замеченные упущения с их стороны;

хранить свои реквизиты доступа к ОИС (логины и пароли) в секрете;

помнить свои реквизиты доступа (в частности имя пользователя или логин для доступа к ОИС, ИР и ИС);

не пытаться работать на рабочих машинах других пользователей или под учетными записями других пользователей без разрешения непосредственного руководителя и информирования СИТ. После предоставления своих реквизитов доступа другим пользователям БГЦА, следует изменить пароль.

При необходимости изменения/добавления рабочих файлов в ИР (например, в ИР BSCA), по возможности следует работать с данными файлами у себя на ПК (файлы, которые ведутся самим пользователем). После завершения работы с файлом его необходимо копировать на ИР. Данная мера позволит иметь как минимум одну резервную копию на ПК пользователя, а при разрыве соединения с ИР – не потерять несохраненную информацию.

**5.11** Пользователям Предприятия запрещается:

использование личных СВТ и мобильных устройств (мобильные телефоны, планшеты и т.п.) для передачи и хранения служебной информации;

подключать (подсоединять) личные мобильные устройств (мобильные телефоны, планшеты, камеры и т.п.) к ПК;

оставлять незаблокированный ПК без присмотра после авторизации в ОС. Если необходим уход от ПК на расстояние, предполагающее выпадение из зоны видимости закрепленного компьютера, следует заблокировать его с помощью комбинации Win+L, либо Сtrl+Alt+Del –> Блокировать компьютер/Заблокировать (надпись может отличаться в зависимости от установленной ОС), а при завершении работы с ПК – выключать его;

создавать помехи при работе с ОИС другим пользователям;

совершать неавторизованную работу с ОИС (самостоятельно осуществлять подключение СВТ, не принадлежащего Предприятию, к ИС Предприятия);

самостоятельно пытаться получить привилегированные права доступа, повысить права доступа на ПК;

скачивать (сбрасывать), открывать информацию из неизвестных подозрительных источников;

работать не под своей учетной записью;

осуществлять обработку информации ограниченного распространения на ПК в информационной сети предприятия, либо на непредназначенных для этого ПК, а также в присутствии посторонних (не допущенных к данной информации) лиц;

оставлять без личного присмотра на рабочем месте или где бы то ни было свой НКИ, а также съемные носители информации, содержащие конфиденциальную информацию;

небрежно относиться к конфиденциальности собственных идентификационных реквизитов (в частности, паролей и прочих кодов авторизованного доступа), вывешивать данные об именах пользователей и их паролях на всеобщее обозрение, предоставлять в общий доступ;

самостоятельно устанавливать ПО на ПК, модифицировать, тестировать, производить поиск и умышленно использовать недокументированные свойства и ошибки в ПО или в его настройках;

вскрывать корпуса СВТ;

предоставлять СВТ, подключенные к ИС Предприятия посторонним без согласования с СИТ и постоянного контроля;

отключать/блокировать антивирусное ПО;

выполнять поиск средств и методов повреждения, уничтожения ОИС, ИС и ИР или преодоления их защиты, а также использовать указанные средства;

использовать на ПК постороннее ПО, предназначенное для сокрытия действий пользователя;

выносить за пределы предприятия СВТ, документированную информацию или ПО без соответствующего разрешения непосредственного руководителя, за исключением служебной необходимости.

использовать съемные носители информации, без проверки указанных носителей антивирусным ПО на своём рабочем ПК.

**5.12** Права пользователей:

получать доступ к ИС, ИР и ОИС для исполнения своих должностных обязанностей в рамках предоставленных им полномочий;

получать консультации от работников СИТ по работе с ИС, ИР и ОИС Предприятия, только после изучения соответствующих инструкций;

оставлять заявки в СИТ, в случае необходимости получения\изменения доступа к ОИС, ИС и ИР Предприятия.

**5.13** Ответственность за исполнение настоящего положения возлагается на всех пользователей. Мера ответственности пользователей системы за действия, совершенные в нарушение установленных требований, определяется размером причиненного ущерба и другими факторами, устанавливаемыми руководством предприятия.

# **6** **ОСНОВНЫЕ ПОЛОЖЕНИЯ**

**6.1** В ИС Предприятия в соответствии с Законом Республики Беларусь «Об авторском праве и смежных правах» применяется только свободно распространяемое либо лицензионное ПО.

**6.2** Успешное и эффективное решение задач обеспечения ИБ достигается путем формирования системы ЛПА, политик, инструкций, положений, правил, регламентов и функциональных обязанностей пользователей. Требования по правовому обеспечению ИБ предусматриваются во всех ЛПА, начиная с Устава предприятия и заканчивая функциональными обязанностями каждого пользователя.

**6.3** К ЛПА по обеспечению ИБ относятся:

* политика по обеспечению ИБ;
* положение о порядке обеспечения ИБ;
* иные документы, содержащие требования по ИБ.

# **7 ЦЕЛИ И ЗАДАЧИ ОБЕСПЕЧЕНИЯ ИБ**

**7.1** Основной целью обеспечения ИБ Предприятия является защита его интересов при создании, изменении и работе с информацией в ИС и ИР от возможного нанесения им недопустимого ущерба посредством незаконного использования, случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных ресурсов и систем Предприятия, а так же её объектов или несанкционированного доступа к передаваемой, обрабатываемой или хранящейся в них информации.

Указанная цель достигается посредством обеспечения и постоянного поддержания следующих свойств активов Предприятия:

обеспечения правового режима использования информационных ресурсов и систем Предприятия, а также ОИС как объектов собственности (служебная информация, ОИС, информация организаций, с которыми осуществляется информационное взаимодействие);

доступности информационных ресурсов, систем Предприятия и ОИС, а также (устойчивого функционирования ИС и ИР, при котором пользователи для исполнения своих обязанностей имеют возможность получения необходимой им информации и результатов ее обработки за приемлемое время);

разграничения прав доступа по категориям пользователей, пользователям и объектам размещения информации;

целостности информации (сохранения содержания и однозначности интерпретации в условиях случайных и/или преднамеренных воздействий) и аутентичности (подтверждение авторства), хранимой в ИР, хранимой и обрабатываемой в ИС Предприятия, а также передаваемой по каналам связи;

конфиденциальности информации, хранимой, обрабатываемой и передаваемой по каналам связи;

эффективного использования и управления активами Предприятия.

**7.2** Достижение основной цели обеспечения ИБ осуществляется путем решения следующих задач:

обеспечение соответствующего требованиям нормативных правовых актов РБ порядка обработки и хранения документированной информации, содержащей сведения, подлежащие защите;

разграничение и контроль физического доступа к объектам защиты ИС предприятия;

разграничение доступа к ИС и ее объектам осуществляется с помощью средств управления правами доступа к информационным активам. Перечень указанных средств содержится в ПЛ СМ 9.4.1;

защита от вмешательства в процесс функционирования ИС предприятия;

предотвращение доступа неавторизованных пользователей и разграничение доступа аутентифицированных пользователей к ИС Предприятия в целом, так и к ОИС;

защита ОИС Предприятия от случайного физического воздействия, в результате которого может произойти нарушение конфиденциальности, целостности и доступности информации;

обеспечение доступности информации в случаях преднамеренных воздействий на объект с целью отказа в обслуживании пользователей ИС и ИР, отказа оборудования ИС Предприятия, в том числе технологического (систем кондиционирования и электропитания);

защита информации предприятия, хранимой в ИР и ИС, обрабатываемой в ИС предприятия, а также передаваемой по каналам связи, от искажения и утечек;

регистрация действий пользователей при использовании защищаемых ресурсов в электронных системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов специалистами СИТ;

своевременное обнаружение и деактивация вредоносного ПО, предотвращающее нарушение конфиденциальности, целостности и доступности информации указанным ПО;

в случае выявления недостатков в ОИС Предприятия с последующей реализацией адекватных мер реагирования;

своевременное выявление источников угроз ИБ, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы ИБ и негативные тенденции;

создание условий для минимизации и локализации возможного ущерба, наносимого неправомерными действиями физических и юридических лиц, снижение негативного влияния и ликвидация последствий нарушения безопасности информации.

**7.3** Обеспечение ИБ Предприятия базируется на принципах:

* законности;
* разумной достаточности;
* гибкости системы защиты;
* персональной ответственности и минимизации полномочий;
* обязательности контроля.

**7.4** Уровень затрат на обеспечение ИБ соответствует величине возможного ущерба от неправомерных воздействий. При этом выбирается тот достаточный уровень защиты, при котором соотношение затрат, рисков и размера возможного ущерба были бы оптимальными и приемлемыми для предприятия.

**7.5** Для обеспечения возможности варьирования уровнем защищенности, система защиты обладает определенной гибкостью, позволяющей обеспечивать необходимый в данный момент уровень безопасности без принятия кардинальных и, соответственно, затратных мер по полному обновлению средств защиты.

**7.6** Распределение прав и обязанностей строится таким образом, чтобы в случае любого нарушения можно было максимально точно идентифицировать ответственного.

**7.7** Попытки нарушения установленных правил обеспечения ИБ своевременно выявляются и пресекаются с использованием СЗИ.

**7.8** Контроль за деятельностью любого пользователя и в отношении любого объекта защиты осуществляется на основе применения средств оперативной регистрации и охватывает как несанкционированные, так и санкционированные действия пользователей.

**7.9** Анализ рисков нарушения безопасности ИР и ИС обязаны проводить специалисты по внутреннему аудиту с участием СИТ и при необходимости с привлечением сторонней организации или экспертов.

**7.10** С целью проверки организации ИБ, а также предупреждения и своевременного выявления случаев ее нарушения ЛПА работниками СИТ в соответствии с выполняемыми функциями проводится контроль состояния ИБ, такой как (ежедневный контроль, выборочные мониторинги, и т.д.) путём анализа сообщений системы мониторинга, системных журналов, поступающих заявок от пользователей.

# **8 ОРГАНИЗАЦИЯ РАБОТЫ С ОИС ПРЕДПРИЯТИЯ**

**8.1** Работа ПК в ИС предприятия осуществляется по правилам, установленным в ЛПА по обеспечению ИБ**.**

**8.2** Обеспечение ИБ включает комплекс повседневно проводимых мероприятий, а именно:

* допуск (предоставление прав доступа) к информации, ОИС и в помещения;
* доступ к информации, ОИС и в помещения в соответствии с предоставленными правами;
* использование СЗИ;
* контроль состояния ИБ;
* действия в случае выявления нарушений ИБ.

**8.3** Инструкция об организации доступа в сеть Интернет, а также рекомендации по безопасному его использованию изложены в Приложении 1.

**8.4** Инструкция об организации работы и использованию электронной почты, а также рекомендации по безопасному её использованию изложены в Приложении 2.

**8.5** При возникновении угрозы ИБ в ИС предприятия либо при возникновении инцидента, связанного с возможностью утечки информации, СИТ осуществляет отключение соответствующих ОИС от ИС. О серьезных уровнях угрозы ИБ, а также инцидентах, связанных с утечкой информации из ИС, СИТ незамедлительно информирует директора Предприятия. При необходимости директор информирует Госстандарт и ОАЦ.

**8.6** Перечень возможных инцидентов ИБ и порядок действий при их возникновении приведен в Приложении 3.

**8.7** Решение инцидентов ИБ ответственными исполнителями СИТ обладает высшим приоритетом.

**8.8** Все инциденты ИБ регистрируются ответственными исполнителями СИТ в системе обработки заявок на техническую поддержку Предприятия.

**8.9** все ПК, работающие в ЛВС организации, должны быть оснащены предустановленным лицензионным (сертифицированным) антивирусным программным обеспечением, имеющим сертификат соответствия Национальной системы подтверждения соответствия Республики Беларусь или положительное экспертное заключение по результатам государственной экспертизы, проводимой Оперативно - аналитическом центре при Президенте (далее – ОАЦ). Информация о сертифицированном антивирусном программном обеспечении размещена на сайте ОАЦ (https://oac.gov.by/activity/information-security-tools/technical-and-cryptographic-information-protection/registry-ism).

**8.10** СИТ поддерживает всё антивирусное ПО на Предприятии (в том числе антивирусные базы) в актуальном состоянии.

**8.11** Установка ПО на ПК производится работниками СИТ по заявке пользователя, эксплуатирующего данный ПК, либо по заявке его руководителя.

Устанавливается исключительно лицензионное или свободно распространяемое ПО, необходимое для выполнения пользователем его должностных обязанностей, либо системное ПО в рамках имеющихся в наличии лицензий. Перечень разрешенного для работы ПО приведен в Приложении 4.

При необходимости установки нового ПО следует обосновать эту необходимость. Если требуется приобретение дополнительного ПО\лицензий, следует оформить докладную записку с обоснованием на имя директора, предварительно согласованную с непосредственным руководителем и начальником СИТ.

**8.12** В случае выявления фактов нарушения ИБ после их устранения в обязательном порядке проводится анализ причин, их повлекших, проверка системы ИБ на участках, где подобные нарушения возможны.

**8.13** Регламент по использованию съемных носителей информации (usb–накопители, карты памяти, внешние жесткие диски и т.п.) следующий:

* Съемные носители информации (usb–накопители, карты памяти, внешние жесткие диски и т.п.) используются для переноса данных (текстовые документы, файлы таблиц, презентации, графики, изображения и т.п.) с одного ПК на другой, а также резервного копирования важной информации.
* Сотрудниками организации (за исключением руководителя организации и руководителей структурных подразделений организации, сотрудников СИТ) допускается работа только с зарегистрированными съемными носителями информации;
* Регистрация съемных носителей информации производиться СИТ по заявке от сотрудника;
* На ПК пользователей отключена функция автозагрузки с внешних съемных носителей информации.
* При подключении съемных носителей запускается антивирусный модуль проверки, который при возникновении вирусных угроз автоматически блокирует подозрительный файл и передаёт информационное сообщение в консоль управления антивирусным ПО. Отключать проверку носителя, который перед этим использовался не на ПК Предприятия пользователям запрещено.
* Работниками допускается работа со съемными носителями информации только после проверки таких носителей актуальным антивирусным ПО с обновленными вирусными базами.
* Работникам запрещается запускать ПО с любых съемных носителей информации.
* Все обнаруженные угрозы хранятся в консоли управления антивирусным ПО и отправляются в первых числах месяца в виде отчетов на почту ответственных работников СИТ.

**8.14** Регламент работы с НКИ, следующий:

* НКИ имеют права пользоваться только те пользователи, которым они выданы.
* по окончанию работ с НКИ, пользователь обязан извлечь их из ПК;
* в конце рабочего дня НКИ перемещаются для хранения в запираемые шкафы\шуфляды;
* хранить в тайне личный ключ;
* обеспечивать защиту личного ключа от случайного уничтожения или модификации (изменения);
* не использовать личный ключ, если соответствующий ему открытый ключ отозван или срок действия этого открытого ключа истек;
* отозвать открытый ключ в случае, если тайна соответствующего ему личного ключа нарушена.

**8.15** Рекомендации по обеспечению ИБ при удаленной работе:

* Для удаленной работы используются исключительно ПК Предприятия.
* Использование пользователями СВТ за пределами территории предприятия санкционируется непосредственным руководителем. В случае необходимости, СИТ предоставляет СВТ для удалённой работы из имеющегося резерва. Уровень защиты такого оборудования такой же, как и для оборудования, расположенного на территории БГЦА.
* Не допускается оставлять ПК, с которого осуществляется удалённая работа, без присмотра. Не допускается покидать рабочее место с открытым сеансом удалённого подключения. При необходимости покинуть рабочее место на длительное время необходимо прервать сеанс связи с ИС Предприятия.
* Не допускается использование ПК, с которого осуществляется удалённая работа, посторонними лицами.
* Не допускается хранение на ПК, с которого осуществляется удалённая работа, документы и файлы, не относящиеся к производственной деятельности.
* В случае если в качестве ПК, с которого осуществляется удалённая работа, выступает портативный компьютер, то запрещается подключаться к общедоступным беспроводным сетям wi‑fi.
* При удаленной работе необходимо руководствоваться отраслевыми рекомендациями Госстандарта по работе в сети Интернет и электронной почтой.

# **9 ОБЪЕКТЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

**9.1** Активы Предприятия требующие защиты: ИР, ИС и ОИС, а также информация, содержащаяся в них, а также технологическое оборудование (системы бесперебойного питания, кондиционеры и т.д.).

**9.2** Классификация и управление активами:

Все активы предприятия учитываются. Анализ всех активов ИС предприятия, подлежащих защите, осуществляет СИТ, при содействии руководителей структурных подразделений и всех пользователей. Контроль актуальности и достоверности перечня активов Предприятия осуществляет СИТ. Краткая инвентаризационная опись активов, подлежащих защите, с их классификацией, приведена в Приложении 5.

Классификация (категорирование) активов имеет своей целью обеспечение дифференцированного подхода к обеспечению их безопасности.

При этом классификация (категорирование) активов осуществляется по требованиям целостности (неизменности) и по степени доступности.

Категория целостности (неизменности):

* высокая: информация, несанкционированная модификация (искажение, подмена, уничтожение) или фальсификация (подделка) которой может привести к нанесению значительного ущерба;
* средняя: информация, несанкционированная модификация, подмена или удаление которой может привести к нанесению незначительного ущерба;
* низкая: информация, к обеспечению целостности и аутентичности которой требования не предъявляются.

Категория доступности:

* постоянная: доступ к информации обеспечивается в любое время суток (за исключением времени технического обслуживания и действий непреодолимой силы, либо по обстоятельствам, не зависящим от СИТ или Предприятия;
* высокая: информация доступна без существенных временных задержек (до суток);
* средняя: доступ к информации может обеспечиваться с существенными временными задержками (задержка получения доступа к информации не должна превышать 2-х суток);
* низкая: временные задержки при доступе к информации практически не лимитированы (допустимая задержка получения доступа к информации - 1-2 недели).

# **10 ОСНОВНЫЕ ОРГАНИЗАЦИОННЫЕ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРОПРИЯТИЯ ПО СОЗДАНИЮ И ОБЕСПЕЧЕНИЮ ФУНКЦИОНИРОВАНИЯ СЗИ**

**10.1 Физическая защита и защита активов предприятия от воздействий окружающей среды**

Эксплуатация ОИС Предприятия (за исключением ПК и мобильных устройств, используемых в служебных целях вне территории Предприятия) осуществляется в помещениях, оборудованных замками, средствами сигнализации и постоянно находящимися под охраной или наблюдением, исключающими возможность бесконтрольного проникновения посторонних лиц и обеспечивающим физическую сохранность находящихся в них защищаемых ресурсов.

Серверное оборудование обеспечено источниками бесперебойного питания.

Состояние источников бесперебойного питания регулярно проверяется СИТ в соответствии с рекомендациями завода-изготовителя.

**10.2 Организация и контроль доступа**

ПК и мобильные устройства идентифицируются в ИС Предприятия с помощью уникальных учетных записей в локальном домене, а также IP и MAC-адресов.

Всё управляемое сетевое оборудование настраивается индивидуально, устанавливаются уникальные пароли, отличные от установленных по умолчанию.

С целью защиты данных авторизации при работе с сервисами сети Интернет применяются криптографические протоколы;

В зависимости от решаемых производственных задач работниками СИТ предоставляется доступ к различным ИР, ИС и ОИС предприятия.

Организация предоставления доступа к ИС «Аккредитация» содержится в Приложении 6.

Порядок работы с ИР «BSCA» содержится в Приложении 7.

Первоначально доступ настраивается работниками СИТ при создании учетной записи (применяются доменные групповые политики) при подготовке ПК для нового пользователя (работника, вступившего в должность).

Для ограничения доступа к информационным системам и ОИС используется парольная защита. Инструкция по использованию парольной защиты содержится в Приложении 8.

Управление учетными записями пользователей для доступа к ИР, ИС и ОИС осуществляется централизованно с помощью средств контроллера домена специалистами СИТ.

Лимит количества неудачных попыток ввода пароля для учетных записей в домене ограничен 5 (пятью).

СИТ обеспечивает каждого пользователя информационных систем предприятия (включая работающих удаленно) индивидуальной учетной записью в домене для доступа к ИС БГЦА. Дополнительно обеспечивается доступ к ИС на основе ролей (групп).

Права доступа пользователей, которые, по своим служебным обязанностям, больше не должны иметь доступ к определенным активам информационной сети предприятия, немедленно изымаются СИТ.

Учетные записи уволенных пользователей информационных систем, ресурсов БГЦА подлежат блокировке и смене пароля в конце последнего рабочего дня работника и последующему удалению при отсутствии информации о необходимости дальнейшего использования учетной записи. Блокировка может также осуществляться по истечению заданного периода времени либо по запросу пользователя.

Регламент доступа к настройкам и администрированию ОИС Предприятия содержится в Приложении 11.

СИТ, при осуществлении контроля доступа к веб-приложениям выполняет:

* периодически, но не менее одного раза в неделю мониторинг (просмотр, анализ) функционирования веб-приложения;
* контроль за внешними подключениями к веб-приложению;
* ежеквартальную инвентаризацию учетных записей по веб-приложению, удаление неиспользуемых и неактивных учетных записей.

Порядок функционирования межсетевого экрана содержится в Приложении 9.

Для организации и управления безопасностью сетей применяется логическое разбиение на сегменты, связь между которыми контролируется при помощи средств межсетевого экранирования и(или) средств виртуальных частных сетей.

Все события, связанные с возможным нарушением режима безопасности, автоматически регистрируются в системных журналах протоколирования событий.

Для каждого регистрируемого события при технической возможности регистрируется дата и время события, тип события, идентификатор субъекта и результат (успех или неудача) события.

Контролю и анализу подлежат:

* неудачные попытки доступа к информационным ресурсам, системам и ОИС;
* события авторизации доступа на предмет выявления несанкционированного использования пользовательских идентификаторов;
* выделение и использование ресурсов с привилегированным доступом.

Периодичность, правила доступа и резервного копирования информации содержатся в Приложении 9.

С целью фиксации актуального времени обеспечивается синхронизация системного времени от единого (общего) источника (в качестве источника использовать службу единого времени Белорусского государственного института метрологии (БелГИМ).

**10.3 Разработка, доработка и обслуживание информационных ресурсов, систем и ОИС**

Действующие и тестовые ИС, а также системы и БД для разработки и обучения работе с ИС «Аккредитация» разделяются для уменьшения риска случайного внесения изменений и/или несанкционированного доступа к эксплуатируемому в рабочем порядке ПО, производственным данным и документированной информации.

События, поступающие в форме заявок пользователей либо автоматических сообщений с информационных систем и их объектов регистрируются, анализируются и обрабатываются согласно Порядка осуществления технической поддержки пользователей.

Техническое обслуживание СВТ осуществляется соответствующим образом с целью предотвращения их отказов.

Ремонт оборудования проводится соответствующим образом, с целью предотвращения компрометации информации и повторного отказа (выхода из строя) оборудования.

Ремонт и обслуживание СВТ выполняются только работниками СИТ, либо под контролем работников СИТ. В случае невозможности ремонта силами СИТ СВТ передаются для дальнейшего ремонта в соответствующие сервисные центры с принятием предварительно мер, предотвращающих утечку информации в электронном виде и реквизитов доступа к информационным системам, ресурсам и ОИС.

Перед передачей машинных носителей информации или СВТ, содержащих документированную информацию в электронном виде на ремонт в сервисные центры, либо при передаче на переработку для дальнейшего извлечения драгметаллов выполняется удаление информации с указанных СВТ и сброс настроек до заводских, исключающие возможность восстановления информации с них.

**10.4 Обеспечение непрерывной работы**

**10.4.1** Непрерывность процесса функционирования информационной сети БГЦА и своевременность восстановления ее работоспособности достигается:

* применением различных способов повышения надежности функционирования аппаратурных средств и программного обеспечения;
* эффективным контролем за соблюдением требований по обеспечению непрерывной работы пользователями;
* проведением постоянного анализа эффективности применяемых мер и средств обеспечения непрерывности работы.

**10.4.2** Способы и средства повышения надежности функционирования ОИС включают в себя:

* использование компонент с повышенной надежностью;
* создание комплектов запасных частей и принадлежностей;
* обеспечение СИТ необходимым измерительным оборудованием и инструментами;
* обеспечение требуемых климатических условий функционирования ОИС, рекомендуемых производителями;
* резервирование ОИС, вспомогательного оборудования, каналов связи, электропитания;
* обеспечение резервного и архивного копирования ПО и информации в электронном виде.

**10.4.3** Периодичность, правила доступа и резервного копирования информации содержатся в Приложении 10.

# **11 ПОРЯДОК ПЕРЕСМОТРА ПОЛОЖЕНИЯ**

**11.1** Пересмотр положения осуществляется в соответствии с ежегодной программой разработки и пересмотра документов системы менеджмента БГЦА.

**11.2** Внеплановое внесение изменений в настоящее Положения выполняется в случаях:

* изменения отраслевых рекомендаций Госстандарта;
* изменения стандартов защиты информации;
* изменения законодательства в области ИБ;
* по решению директора БГЦА.

Для удобства использования и актуализации, инструкции представлены в виде приложений.

# **Приложение 1**

Инструкция об организации доступа в сеть Интернет

Настоящая Инструкция описывает порядок организации доступа в сеть Интернет на предприятии.

Подключение компьютеров к сети Интернет осуществляется после подключения их к ЛВС предприятия и аутентификации под учетной записью пользователя, который будет использовать данный ПК (если иное не определено другими ЛПА предприятия, например, Положением о ведении делопроизводства, по документам, содержащим служебную информацию ограниченного распространения).

Ресурсы сети Интернет могут использоваться работниками предприятия только для информационно-аналитической работы в интересах производственной, организационной и хозяйственной деятельности, а также для получения, передачи и распространения информации, связанной с деятельностью БГЦА. Посредством сети Интернет осуществляется доступ к ИС «Аккредитация», электронной почте, онлайн версиям ИПС.

Ответственность за содержание информации, размещаемой (передаваемой) в сети Интернет, несут лица, разместившие (передавшие) эту информацию и владельцы информационных ресурсов.

Пользователи несут персональную ответственность за использование сети Интернет на служебных (корпоративных) мобильных устройствах (мобильные телефоны, планшеты, модемы с корпоративными тарифными планами Интернет-провайдеров).

Правила использования любых ресурсов в сети Интернет определяют владельцы этих ресурсов. Любые действия пользователей предприятия, вызывающие жалобы владельцев или абонентов других сетей, серверов, информационных ресурсов, форумов, конференций и т.п. недопустимы и являются нарушением правил пользования услугами доступа в Интернет.

**При работе в сети Интернет пользователям запрещается:**

* получение, распространение или воспроизведение информации, которая противоречит белорусскому законодательству, не допускается распространение персональных данных, заведомо ложных сведений, порочащих честь и достоинство другого лица или подрывающих его репутацию, оскорбительной информации, включая нецензурную лексику, призывов к насилию, разжиганию расовой или национальной ненависти, порнографии, информации с нарушением авторских прав, хулиганской или мошеннической информации;
* посещение ресурсов, тематика которых не соответствует направлению деятельности сотрудника предприятия (нецелевое использование трафика);
* производить передачу в сеть Интернет конфиденциальной информации, в том числе информации, отнесенной к коммерческой тайне, а также информации, которая может нанести ущерб репутации БГЦА, заявителям на аккредитацию и аккредитованным субъектам, а также Республике Беларусь в целом;
* пользоваться пиринговыми сетями (использовать торрент-клиенты и т.п.);
* подключаться с рабочего места в локальной сети предприятия к сетям связи общего пользования (в том числе к сети Интернет) через другие каналы доступа (мобильный телефон, модем и т.п.), за исключением средств связи, предоставленных пользователям предприятием, заказчиком, арендодателем (точка доступа Wi-Fi (в том числе, посредством мобильного телефона, модемa);
* скачивать видео и аудио файлы, а также использовать потоковое видео или аудио, не соответствующие направлениям деятельности предприятия;
* скачивать программное обеспечение (за исключением работников СИТ);
* пользоваться прокси-серверами, анонимайзерами;
* использование иных протоколов передачи данных в сети Интернет, кроме http, https (просмотр интернет-страниц через браузер), почтовых протоколов: smtp, pop3, imap.

Не относится к СИТ;

* использовать ресурсы сети Интернет, предназначенных для сокрытия действий пользователя;
* пользоваться портативными или иными версиями браузеров, не установленных работниками СИТ;
* использовать электронную почту, доступ к информационным ресурсам, IP-телефонию, социальные сети и публичные системы мгновенных сообщений в личных целях;
* использовать облачные хранилища (Google Drive, Yandex Disk и т.д.) без согласования с СИТ;
* использовать IP-телефонию, социальные сети (Facebook, ВКонтакте, Instagram и т.п.) и внешние системы мгновенных сообщений (Viber, Telegram, WhatsApp, Skype, Zoom и т.п.) на ПК и мобильных устройствах Предприятия;

Учет использования ресурсов сети Интернет-пользователями осуществляется с помощью программно-аппаратного комплекса «шлюз информационной безопасности» (межсетевым экраном), с помощью которого реализуются функции защиты сетевых соединений, межсетевое взаимодействие.

Информация об используемых пользователями организации ресурсах сети Интернет автоматически протоколируется межсетевым экраном и хранится в электронном виде не менее 1 года и анализируется на постоянной основе администратором системным, либо работником СИТ, исполняющим его обязанности.

При уличении работника БГЦА в систематическом либо продолжительном нецелевом использовании сети Интернет информация об это передаётся комиссии по контролю за использованием работниками БГЦА сети Интернет и корпоративной электронной почты.

Шлюз информационной безопасности осуществляет фильтрацию трафика и блокирует сервисы, которые относятся к нецелевому, запрещенному или вредоносному Интернет-трафику. В сети предприятия используются DNS сервера РУП «Белтелеком» и включен фильтр №7 (фильтр оператора+DNS+AV+IPS TCP: 21, 22, 23, 25, 53, 69, 80, 110, 119, 123, 443, 444, 465, 587, 993, 995, >1024; UDP: 53, 69, 123, 444, 465, 500, 993, >1024) для дополнительной фильтрации.

Отчёты, содержащие информацию об использовании работниками предприятия сети Интернет, формируются и передаются на рассмотрение Комиссии по контролю за использованием работниками БГЦА сети Интернет (далее – Комиссия) согласно Положению о комиссии по контролю за использованием работниками сети Интернет.

Доступ к ресурсам сети Интернет может быть заблокирован работниками СИТ без предварительного уведомления, при возникновении нештатных ситуаций, либо в иных случаях нецелевого или незаконного использования сети Интернет.

Предварительное отнесение Интернет-трафика к нецелевому осуществляется администратором системным самостоятельно на основе анализа содержания посещенных пользователями Интернет-сайтов, затем информация передается на рассмотрение Комиссии с целью принятия окончательного решения и выработки дальнейших мер.

# **Приложение 2**

Инструкция об организации работы и использованию электронной почты

Настоящая инструкция определяет порядок создания и правила использования пользователями корпоративной электронной почтой предприятия (далее – электронной почтой), их права и обязанности с целями обеспечения ИБ, предотвращения утечки информации, эффективного использование электронной почты в интересах предприятия.

1. Использование электронной почты не должно противоречить законодательству Республики Беларусь.
2. Содержимое почтовых сообщений может быть раскрыто с санкции руководства или по требованию правоохранительных органов с целью обеспечения информационной безопасности, пресечения нарушения законодательства Республики Беларусь, предотвращения утечки информации.
3. Пользователи несут персональную ответственность за использование электронной почты на служебных (корпоративных) мобильных устройствах (мобильные телефоны, планшеты, модемы с корпоративными тарифными планами Интернет-провайдеров).
4. Электронная почта предназначена для:
* оперативного обмена служебной информацией, в том числе файлами между работниками предприятия (в случае невозможности обмена посредством сетевого ресурса BSCA);
* рабочей переписки с Госстандартом и другими организациями по вопросам текущей деятельности;
* рабочей переписки в рамках осуществления международной деятельности;
* рассылки необходимой информации участникам процесса аккредитации и заявителям\претендентам;
* рассылка необходимой информации заявителям на тренинги;
* рассылки информации о времени и повестке совещаний, а также подготовительных материалов при невозможности отправки посредством корпоративной системы обмена мгновенными сообщениями (Spark);
* рассылки напоминаний о событиях и мероприятиях (автоматически, а также в ручном режиме при невозможности отправки посредством корпоративной системы обмена мгновенными сообщениями (Spark).

**5** Адреса электронной почты и почтовые базы данных (содержимое электронных почтовых ящиков) являются собственностью предприятия. Содержимое любого электронного почтового ящика может быть проверено с помощью работников СИТ без предварительного уведомления пользователей.

**6** Все электронные почтовые сообщения должны отправляться пользователями только с корпоративных электронных почтовых ящиков, за исключением случаев, когда электронная почта недоступна, либо не может использоваться по причинам имеющихся ограничений (например, при массовых рассылках). Сторонние почтовые сервисы запрещено использовать для обмена информацией, распространение и (или) предоставление которой ограничено.

**7** С целью обеспечения защиты информации корпоративные почтовые ящики пользователей располагаются на внешних почтовых серверах в зоне защищенного хостинга, предоставляемых уполномоченным поставщиком интернет-услуг (домен – bsca.by). Доступ к электронной почте осуществляется посредством сети Интернет, по адресу: https://bsca.by/roundcube/ либо с помощью почтовых клиентов, устанавливаемых и настраиваемых работниками СИТ.

**8** Индивидуальные почтовые ящики для работников организации создаются в следующем формате: «первая буква имени».«фамилия»@«домен», где «первая буква имени», «фамилия» – латинская транскрипция фамилии пользователя (например: i.ivanov@bsca.by).

**9** Каждый пользователь имеет право на открытие индивидуального электронного почтового ящика.

**10** Размер индивидуального электронного почтового ящика пользователя составляет 500Мб (может быть увеличен, при условии наличия технической возможности) в пределах свободного места на почтовом сервере. Пользователь самостоятельно следит за лимитом индивидуального электронного почтового ящика и в случае необходимости удаляет/архивирует письма;

**11** Основной официальный адрес электронной почты предприятия: bsca@bsca.by (является аналогом обычного почтового адреса). Электронные обращения направляются лицами непосредственно на адрес электронной почты bsca@bsca.by либо с использованием специальных форм на сайте. Информация об этом содержится на официальном сайте Предприятия.

**12** В случае необходимости, может быть создан электронный почтовый ящик подразделения. Область применения указанного ящика: в случае, если общую функцию выполняют несколько работников подразделения с целью обработки входящих сообщений любым из работников подразделения.

**13** Порядок работы с электронными почтовыми ящиками, следующий:

* работники СИТ создают электронный почтовый ящик и устанавливают пароль в соответствии с Инструкцией по использованию парольной защиты всем новым пользователям при поступлении информации о принятии нового работника, который будет являться пользователем;
* работники СИТ выдают реквизиты для доступа к индивидуальному почтовому ящику всем новым пользователям;
* для создания электронного почтового ящика подразделения или группы работников, руководитель подразделения подает заявку в СИТ;
* для смены или восстановления забытого пароля пользователю либо его непосредственному руководителю необходимо подать заявку в СИТ;
* при увольнении пользователя доступ к его электронному почтовому ящику со стороны пользователя прекращается путем назначения нового пароля. В случае наличия информации в электронном почтовом ящике, указанный пароль передается непосредственному руководителю пользователя с целью сохранения необходимых электронных почтовых сообщений. Максимальный срок, после которого ящик удаляется, составляет 1 месяц. В случае необходимости, контактам указанного электронного почтового ящика пользователем либо его непосредственным начальником осуществляется отправка уведомления о прекращении использования текущего электронного почтового ящика;
* почтовое ПО или web-интерфейс у пользователей должен быть активен в течение всего рабочего дня.
* с целью обеспечения ИБ и защиты от спама не рекомендуется размещать свой адрес электронной почты, либо адреса электронных почтовых ящиков других пользователей на общедоступных ресурсах Интернет (сайты, форумы, конференции и т.п.);
* пользователям следует обращать свое внимание на подозрительные письма и работать с ними, согласно признакам и алгоритму обработки подозрительных сообщений.
* Дополнительно все письма в автоматическом режиме проверяются антивирусным ПО, установленным на ПК пользователей. На почтовом сервере установлена фильтрация спам рассылок и нежелательной почты.
1. В случае временного замещения одного пользователя другим, следует обращаться в СИТ для установки переадресации;
2. При подозрении работника БГЦА в нецелевом использовании электронной почты на предприятии инициируется служебная проверка, проводимая комиссией по контролю за использованием работниками БГЦА сети Интернет и корпоративной электронной почты.
3. Пользователями почтовых ящиков, а также, в случае необходимости, работниками СИТ, должна осуществляться идентификация признаков подозрительных входящих электронных сообщений:
	* письмо получено от неизвестного ранее адресата, подписано неизвестным или, наоборот, известным лицом (организацией), с которым переписка ранее не велась (например: MeganFox@, KRonaldo@, EADS@ и т.д.) либо на вымышленных почтовых сервисах (например: @63x423.mail.ru, @se8t5ghz.mailmarket.ru);
	* письмо содержит следующую информацию: временные параметры, требующие принятия срочного решения (обороты: «срочно», «не терпит отлагательств» и т.д.); пароль для доступа к вложенному файлу; наличие у отправителя каких-либо проблем со связью с получателем (то есть объяснение того, что получатель не знает, с кем имеет дело), с выполнением работ, с отправкой грузов, с получением документов и т.д.; описание проблемного вопроса материального характера (денежная транзакция, поставки/закупки, создание инвестиционных фондов, денежный выигрыш, пожертвование и т.д.);
	* письмо имеет вложенные файлы форматов doc/docx, xls/xlsx, rtf, pdf, jpg, jpeg, zip, rar, js, exe, bat, vbs, py, sh, gz;
	* сообщение содержит ссылки HTML (не рекомендуется осуществлять переход по указанным ссылкам, даже если отправитель вам знаком (за исключением размещения информации на известных облачных хранилищах);
	* письмо содержит графические изображения либо виртуальные кнопки, требующие загрузить какие-либо широко распространенные приложения или обновить их для просмотра содержимого. Совершать предлагаемые действия запрещено (вид у виртуальных кнопок или графических изображений может быть аналогичен известным приложениям);
	* в случае невозможности однозначной идентификации подозрительного письма необходимо оставить заявку в СИТ и не открывать вложения\не переходить по ссылке до получения ответа. В случае необходимости работники СИТ информируют Национальный центр реагирования на компьютерные инциденты.

**При работе с электронной почтой пользователям запрещается:**

1. использовать сервисы корпоративной электронной почты на сторонних ПК и мобильных устройствах;
2. использовать электронную почту в целях, не связанных с их функциональными обязанностями в БГЦА (личных целях, либо для получения коммерческой выгоды);
3. использовать почтовый адрес для регистрации на различных ресурсах в сети Интернет, направленность которых не связана с производственной деятельностью БГЦА;
4. использование адреса электронной почты для оформления подписки на периодическую рассылку материалов из сети Интернет, не связанных с исполнением служебных обязанностей;
5. использовать несуществующие обратные электронные адреса при отправке электронных писем;
6. игнорировать либо отключать предупреждения средств антивирусной защиты при открытии вложенных файлов во входящих сообщениях электронной почты, даже если отправитель письма хорошо известен;
7. осуществлять массовую рассылку электронных почтовых сообщений без согласования со своим непосредственным руководителем и СИТ;
8. осуществлять массовую рассылку электронных почтовых сообщений рекламного характера;
9. работа с ящиками электронной почты, находящимися на бесплатных почтовых серверах в сети Интернет;
10. распространять информацию ограниченного распространения (конфиденциальную и относящуюся к коммерческой тайне);
11. предоставление другим пользователям и третьим лицам в пользование свой электронному почтовый ящик, либо реквизитов доступа к нему, если всё же пароль предоставлялся кому-то, то после этого следует оставлять заявку в СИТ для осуществления смены пароля;
12. открывать письма, полученные от неизвестного ранее адресата, подписанные неизвестным или, наоборот, известным лицом (организацией), с которым переписка ранее не велась (например: MeganFox@, KRonaldo@, EADS@ и т.д.);
13. осуществлять переход по гиперссылкам, размещенным в письме, полученном от неизвестного ранее адресата (за исключением размещения информации на известных облачных хранилищах);
14. открывать письма, содержащие:
	* в теме или содержании информацию о выигрышах/переводах или с просьбами срочно ознакомиться/подписать/ответить (полученными от неизвестного адресата);
	* пометку RE (ответ на полученное письмо), если вы не отправляли письмо указанному адресату ранее;
	* если электронный почтовый адрес размещен на почтовом сервере @bsca.by, но в качестве отправителя указан несуществующий/неизвестный пользователь (copier@bsca.by т.п.). *Справочно: Все имена пользователей корпоративной электронной почты, за исключением: admin, brest, bsca, buh, dev, gomel, mogilev, kalinkovichi, postmaster, support, system, trening, vitebsk@bsca.by заданы в следующем формате: первая буква имени и фамилия латинскими буквами, разделенные точкой “.” (**o.shafranskaya**,* *z.kroman@bsca.by* *и т.д.).*
15. открывать прикрепленные к электронному письму файлы, если письмо:
	* получено от неизвестного адресата;
	* содержит графические изображения либо виртуальные кнопки, требующие загрузить какие-либо широко распространенные приложения или обновить их для просмотра содержимого;
	* сообщение содержит графические изображения либо виртуальные кнопки, требующие загрузить какие–либо широко распространённые приложения или обновить их для просмотра содержимого. Совершать предлагаемые действия запрещено (вид у виртуальных кнопок может быть аналогичен известным приложениям).

 **31** Рекомендации к оформлению электронных сообщений и правила эффективной работы с электронной почтой

При оформлении электронных сообщений рекомендуется использовать в организации следующие подходы:

1. При оформлении электронного сообщения необходимо заполнять следующие поля:

адрес получателя;

тема электронного сообщения;

текст электронного сообщения (при необходимости, могут быть вложены различные файлы);

подпись отправителя.

2. Формат подписи отправителя:

С уважением,

<фамилия имя>;

<должность>;

<структурное подразделение Организации>;

<наименование Организации>;

<адрес>;

<номера телефонов, мессенджеры, адреса электронной почты>;

<сайт>.

3. В почтовом клиенте существует возможность создания подписи и автоматической вставки ее в электронное сообщение. При необходимости можно создать несколько подписей для различных получателей.

4. При формировании ответов на полученные электронные сообщения можно использовать упрощенную подпись.

5. При работе с электронной почтой рекомендуется соблюдать следующие правила:

при написании писем руководствоваться общими правилами ведения деловой корреспонденции, т.е. письмо должно содержать обращение к получателю, подпись отправителя, заполненное поле «Тема». В письме должны быть исправлены грамматические ошибки;

в параметрах почтовой программы включить опцию оповещения при получении нового письма;

в параметрах почтовой программы включить опцию отправки уведомления на запрос о доставке;

отвечать на письма, требующие ответа в течение суток. Если письмо требует для подготовки ответа больший срок, в течение суток отправляется ответ, в котором указывается срок отправки полного ответа;

для ответа на письмо пользоваться командой «Ответить», чтобы облегчить получателю понимание темы и сути письма;

в письмах, содержащих поручения, просьбы, и директивные указания, в поле «Кому» указывать только тех, к кому это обращено. Если необходимо дополнительно проинформировать кого-либо о содержании письма, адрес такого получателя вносится в поле «Копия»;

хранить принятые и отправленные служебные сообщения

не менее 6 месяцев;

для хранения сообщений использовать возможности почтовой программы по созданию иерархии папок, аналогично организации файловой структуры MS Windows;

использовать папку «Входящие» как контрольный лист, и оставлять в ней необработанные сообщения.

6. Рекомендуется создать под каждый проект, категорию отдельные папки. Это поможет быстро найти нужную информацию.

7. Активно использовать применение ярлыков, отметок цветом. Это сделает заметным для визуального восприятия сортировку писем.

8. Досконально изучить и знать систему настроек в почтовом аккаунте. Это поможет эффективно ею управлять.

9. Следует отписаться от неактуальных рассылок.

10. При работе с письмами рекомендуется рассортировать все письма по категориям, специфике и важности. В папке «Входящие» можно оставлять письма, которые требуют немедленного или скорого ответа. Их также можно сразу отметить цветными метками или ярлыками.

11. Рекомендуется структурировать исходящие письма. Для этого можно присваивать им ярлыки или метки, так они быстрее найдутся в нужный момент. Можно создать папки для самых важных из них и использовать перемещение.

12. Рекомендуется разделять письма по степени важности и срочности: срочные – неважные; срочные – важные; несрочные –неважные: несрочные – важные. Важные письма, которые требуют ответа или определенной работы сегодня, можно оставлять в папке «Входящие», после выполнения работы перемещать в соответствующую папку.

# **Приложение 3**

Порядок действий по устранению инцидентов ИБ

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Инциденты ИБ** | **Действия****пользователей** | **Действия работников СИТ** |
|  | 1 | 2 | 3 |
| 1 | Системные сбои или перезагрузки | Оставить заявку в СИТ | Провести анализ журналов регистрации ошибок. Принять меры к устранению инцидента в соответствии с кодом ошибки |
| 2 | Ошибки у пользователей | Оставить заявку в СИТ | Принять меры к устранению последствий ошибки. При необходимости восстановить данные из резервных копий. |
| 3 | Несоблюдение правил ИБ | Оставить заявку в СИТ | Сообщить о нарушении непосредственному начальнику работника, несоблюдающему правил ИБ. При необходимости принять меры к блокировке учетной записи пользователя, нарушающего правила ИБ |
| 4 | Нарушение физических мер защиты серверного и сетевого оборудования | Немедленно сообщить об инциденте в СИТ и начальнику АХГ | Совместно с начальником АХГ восстановить физическую защиту серверного и сетевого оборудования |
| 5 | Неконтролируемые изменения в операционной системе ПК | Немедленно сообщить об инциденте работникам СИТ | Установить причину инцидента. Принять меры к восстановлению нормальной работоспособности систем. При необходимости восстановить данные из резервных копий резервных копий |
| 6 | Сбои и отказы СВТ и ПО | Оставить заявку в СИТ | Установить причину сбоя программного обеспечения. Принять меры к устранению указанных инцидентов. В случае отказа технических средств принять меры по восстановлению их работоспособности |
| 7 | Подозрение на возможность несанкционированного доступа к ПК работника | Немедленно сообщить об инциденте работникам СИТ | Принять меры по устранению несанкционированного доступа. Проанализировать причины возникновения инцидента и принять меры к недопущению повторов данного инцидента |
| 8 | Вероятность возникновения вирусной угрозы | Отключиться от ЛВС или информационной системыПопытаться устранить заражение имеющимися в наличие антивирусными средствами. В случае невозможности устранения собственными силами сообщить работникам СИТ | Принять меры к отключению «зараженного» ПК от информационной системы. Проанализировать вид вредоносного ПО. Устранить последствия вирусной атаки. Проанализировать причины возникновения инцидента и принять меры к недопущению повторов данного инцидента |
| 9 | Подозрение на вредоносную рассылку в сообщении электронной почты | Действовать согласно Инструкции об организации работы и использованию электронной почты | В случае получения заявки, работникам СИТ провести анализ полученных писем на предмет наличия в них вредоносных файлов и ссылок |
| 10 | Возникновение нештатной ситуации (сбои, повреждения и отказы) ИР и ИС | Немедленно сообщить об инциденте работникам СИТ | В случае необходимости – блокируют доступ к ИС и\или ИР всем либо отдельным пользователям.Информируют пользователей о проводимых работах (в случае блокировки систем)Принимают все необходимые меры по восстановлению состояния систем до инцидента произошедшего инцидента.Проанализировать причины возникновения инцидента и принять меры к недопущению повторов данного инцидента |

# **Приложение 4**

Перечень разрешенного для работы ПО

|  |  |
| --- | --- |
| **Назначение ПО** | **Вид ПО** |
| Обеспечение взаимодействия аппаратных и программных частей ПК между собой, а также взаимодействие пользователя и ПК | Операционная система с набором необходимых драйверов (Microsoft Windows) |
| Антивирусная защита ПК | ПО для антивирусной защиты ПК (Kaspersky Lab) |
| Автоматизация делопроизводства, взаимодействие с СМДО | ПО электронного документооборота совместимое с форматом СМДО (SMBusiness) |
| Автоматизация обработки электронной почты | Почтовый клиент (Thunderbird или MS Outlook) |
| Автоматизация обработки текстовой информации, таблиц, презентаций, диаграмм | Офисные пакеты (Microsoft Office) |
| Автоматизация обработки электронных документов в формате PDF | ПО для работы с форматом PDF (Adobe Acrobat, Foxit Reader) |
| Обработка электронных документов, содержащихся в архивах. | ПО для работы с архивами (WinRAR – shareware версия) |
| Клиент для удаленного подключения к локальной сети предприятия | CheckPoint Endpoint Security |
| Клиент системы обмена мгновенными сообщениями | Spark |
| Информационно-поисковые системы | ИПС «ЭТАЛОН», ИПС Стандарт |
| Браузеры | Сhrome, Mozilla, Opera, Yandex Browser |
| Бухгалтерские системы | 1С:Предприятие |
| Криптография и менеджмент сертификатов | Персональный менеджер Avest |

В зависимости от решаемых производственных задач перечень ПО, устанавливаемого на ПК, может быть расширен (в рамках имеющихся лицензий либо свободно распространяемым ПО).

# **Приложение 5**

Краткая инвентаризационная опись активов предприятия

1. **ОИС:**
	1. **СЗИ:**
	* Шлюз ИБ: межсетевой экран CheckPoint;
	* Антивирус Kaspersky Endpoint Security.
	1. Сервера;
	2. Сетевые накопители (NAS);
	3. Персональные компьютеры (ПК) и мобильные устройства;
	4. Печатающие и сканирующие устройства;
	5. Коммутаторы, маршрутизаторы, медиаконвертеры, модемы, система видеоконференцсвязи (ВКС).
	6. **Программное обеспечение:**
	* Антивирус Kaspersky Endpoint Security;
	* Управление шлюзом безопасности CheckPoint;
	* Операционные системы семейства Windows;
	* Информационно-поисковые системы (ИПС «Стандарт», «ЭТАЛОН»);
	* Решение для автоматизации бухгалтерского учёта 1С: бухгалтерия;
	* Решение для автоматизации расчёта зарплаты и управления персоналом 1С: Зарплата (1С: ЗУП»);
	* Система электронного документооборота «SMBusiness»;
	* Система управления базами данных (СУБД) «MS SQL»;
	* Ignite Realtime: Openfire – корпоративный IM-сервер для организации эффективной системы обмена мгновенными сообщениями и документами;
	* Открытая система обработки заявок на техническую поддержку БГЦА OTRS;
	* Открытое серверное веб-приложение для управления проектами и задачами (в том числе для отслеживания ошибок) Redmine;
	* Открытое решение распределенного мониторинга корпоративного класса Zabbix.
2. **ИС «Аккредитация»:**
	* ИР «Реестр НСА» (включая национальную часть Единого Реестра ООС ЕАЭС);
	* ИР «Реестр экспертов по аккредитации».
	* ИР «BSCA» – информационный ресурс, содержащий документированную информацию и материалы БГЦА в электронном виде, расположенный в ЛВС предприятия.

**Классификация активов БГЦА**

**По наличию (доступности - Д):**

1. Критический – без них работа предприятия фактически останавливается (Д0):
	* ИС «Аккредитация»;
	* Шлюз ИБ»;
	* 1С «Бухгалтерия».
2. Очень важный – без них можно работать, но очень короткое время (Д1):
	* Серверное оборудование и накопители;
	* Коммутаторы и прочее сетевое оборудование;
	* ПК.
3. Важный – без него можно работать некоторое время, но рано или поздно он понадобится (Д2):

Печатающие устройства.

4. Полезный - без них можно работать, но его использование экономит ресурсы (ДЗ):

* + Ignite Realtime: Openfire;
	+ OTRS;
	+ ИПС «ЭТАЛОН»;
	+ Zabbix.
1. Несущественный - устаревший или неиспользуемый, не влияющий на работу предприятия (Д4): нет

**По несанкционированной модификации (целостность):**

* + Критический: его несанкционированное изменение приведет к неправильной работе всего предприятия или значительной его части (Ц0).
	+ Очень важный: его несанкционированное изменение приведет к неправильной работе предприятия через некоторое время, если не будут предприняты некоторые действия (Ц1).
	+ Важный: его несанкционированное изменение приведет к неправильной работе части предприятия через некоторое время, если не будут предприняты некоторые действия (Ц2).
	+ Значимый: его несанкционированное изменение скажется через некоторое время, но не приведет к сбою в работе предприятия (ЦЗ).
	+ Незначимый: его несанкционированное изменение не скажется на работе системы (Ц4).

# **Приложение 6**

Организация доступа к ИС «Аккредитация»

1. Каждому пользователю назначается одна или несколько ролей доступа. При назначении нескольких ролей доступа права в ролях объединяются. Права назначаются согласно выполняемым пользователем работам.
2. В рамках ИС определены следующие способы доступа зарегистрированных пользователей:
	1. На основе группы ролей администрирования (администратор системы, администратор предприятия, администратор справочников).
	2. На основе группы ролей-операторов программных модулей ("Орган по оценке соответствия", "Эксперт", "Тех. оснащенность", "Реестр МВИ", "Документы международных организаций", "НСИ", "Аналитика" и т.п.).
	3. На основе группы ролей-операторов с разрешенным частичным функционалом в рамках программных модулей (организатор работ по аккредитации (куратор), эксперт, привлекаемый эксперт, сотрудник органа по оценке соответствия).
3. Любые изменения состава и полномочий пользователей подсистем ИС «Аккредитация» производятся либо согласно ЛПА, либо по согласованным с ответственными за программные модули исполнителями со стороны СИТ. Уровень полномочий каждого пользователя определяется индивидуально с соблюдением требования: каждый пользователь получает доступ только к той информации, которая необходима ему для выполнения своих обязанностей.
4. Подробные сведения о доступе к информации каждой роли содержится в Матрице доступа к ИС «Аккредитация». Указанная Матрица постоянно актуализируется по мере изменения прав доступа\доработки ИС «Аккредитация».
5. При предоставлении доступа к ИС «Аккредитация» сторонним организациям/физическим лицам указанные лица обязаны самостоятельно контролировать безопасность выданных учетных записей и информировать БГЦА о несанкционированных доступах, компьютерных вирусных атаках путем уведомления по электронному адреса dev@bsca.by.

# **Приложение 7**

Порядок работы с информационным ресурсе БГЦА (BSCA)

1. Начальники подразделений являются ответственными за содержимое и определение прав доступа к каталогам подразделения, расположенным на ИР BSCA.
2. Управление доступом к ИР BSCA:

При необходимости получения доступа к ИР, доступ к которому ограничен – следует получить разрешение ответственного за данный ИР и направить заявку в СИТ.

**Методические указания и структура информационного ресурса BSCA**

1. Информационный ресурс «BSCA» – сетевой ресурс предприятия, предназначенный для размещения информации общего доступа в электронном виде, с целью ознакомления и использования в работе (ЛНПА, шаблоны, инструкции и пр.), а также для совместной работы с копиями документов в электронном виде, документированной информацией (проектами документов, электронными журналами, базами данных) и мультимедиа информацией подразделений.



1.1 Каталог «Share» (совместное использование) – предназначен для совместной работы подразделений предприятия. Предполагает размещение оперативной информации (рабочих файлов подразделения (журналов, электронных таблиц) и каталогов, ведение которых осуществляет несколько подразделений одновременно происходит на постоянной основе и которые должны быть доступны всем\определенным подразделениям\пользователям, согласно предоставленной ответственными подразделениями информации по форме Приложения 2.

1.1.1 Каталог «Arc\_Share» (совместные файлы, ведение которых прекращено) – предназначен для хранения рабочих файлов архивного характера текущего каталога (по месяцам, по годам). Изменение структуры и замена файлов в данном каталоге доступно только определенному оператору архива (в соответствии с предоставленной информацией). Хранение файлов не архивного характера в указанном каталоге запрещено.

1.2 Каталоги «Dept» (сокр. Department) – предназначен для хранения рабочих файлов подразделения. Для именования используется аббревиатура отдела (например: «СИТ»);

1.2.1 Каталог «In» (сокр. «inbox» – входящие) – предназначен для предоставления файлов\каталогов подразделению. Указанный каталог предназначен только для обмена информацией, не для хранения. Информация в указанном каталоге не резервируется. К указанному каталогу предоставляется полный доступ всем пользователям предприятия. Рекомендуется внутри каталога создать поименованные папки работников текущего подразделения;

1.2.2 Каталог «Private» – предназначен для хранения рабочих файлов\каталогов подразделения без предоставления доступа работникам других подразделений. Рекомендуется внутри каталога создать поименованные папки работников текущего подразделения;

1.2.3 Каталог «Arc\_Dept» – предназначен для хранения рабочих файлов архивного характера подразделения (по месяцам, по годам). Под эту категорию подпадает информация накопительного характера (договора, акты, протоколы, дела и т.п.). Изменение структуры и замена файлов в данном каталоге доступно только определенному оператору архива (в соответствии с предоставленной информацией). Хранение информации не архивного характера в указанном каталоге запрещено.

1.3 Каталог «Temp» (сокращение от «temporary» – временное использование). Каталог, созданный для временного размещения файлов\каталогов, ценность которых не определена (есть сомнения по поводу целесообразности дальнейшего хранения, не определен создатель или ответственный исполнитель информации). Все бесхозные каталоги перемещаются СИТ в данный каталог. По мере необходимости указанный каталог очищается (информация с него удаляется или перемещается на другие средства хранения информации и становится доступна для пользователей только по запросу в СИТ). Резервное копирование информация с данного каталога не осуществляется.

2 При формировании структуры и перемещении информации следует, по возможности, не использовать длинные названия файлов и каталогов на русском языке, в особенности при уже имеющейся большой глубине вложения.

3 Хранение на сервере личной информации (мультимедиа файлы: видео, музыка, семейные фотографии и т.п.) не допускается. Информация, однозначно интерпретируемая как не рабочая будет перемещаться и в последствии удаляться.

**Методические указания по формированию перечня файлов\каталогов информационного ресурса BSCA**

1. Для каталога Share и Dept подразделениям необходимо составить перечень согласно представленному ниже шаблону, содержащий ведения о рабочих каталогах\файлах подразделения и каталогах\файлов, за формирование и ведение которых отвечает подразделение, с указанием полных путей, с определением:
* прав доступа (Подразделения\Пользователи –чтение/добавление/изменение/удаление). Составление списка пользователей, которым будут доступен файл\каталог, с обязательным указанием прав доступа (на чтение\изменение\удаление) пофамильно либо по подразделениям. С целью обеспечения высокого уровня защиты информации права доступа следует определить максимально детально.

После назначения оператора архива от подразделения и переноса информации – изменять, удалять и перемещать данные архивного характера за прошлые периоды будет запрещено. Возможность добавлять новую информацию будет только у назначенного оператора» архивных данных».

1. Вариант с указанием корневой папки и указанием максимальных прав доступа не подходит.
2. В случае необходимости внесения изменений/дополнений в утвержденный (сформированный) Перечень, необходимо в СИТ предоставить актуализированный Перечень с указанными правками. В 3-х дневный срок СИТ выполняет назначение прав доступа и организует резервное копирование информации, согласно полученных от подразделений актуализированных Перечней.
3. Шаблон перечня для формирования подразделениями и последующей передачи в СИТ (сведения внесены в качестве примера):

**«Наименование отдела»**

**Перечень информации для организации доступа и резервирования**

|  |  |  |
| --- | --- | --- |
| **№ п\п.** | **Полное имя файла/папки** | **Права доступа** |
| 1 | w:\!ОИТ\test.txt | Все |
| 2 | w:\!ОИТ\Инструкции | Изменение: СИТЧтение: Все |
| 3 | w:\Share\Arc\_Share\!МАТЕРИАЛЫ ПО ОЦЕНКЕ\BY 1\ | Оператор архива:Иванов И.И.Чтение: Все |
| 4 | w:\!КОМАНДИРОВКИ И РАБОТЫ | Изменение: ОЭПКЧтение: ОАЛ1,2;ООРА |

Начальник отдела «И.О.Фамилия»

# **Приложение 8**

Инструкция по использованию парольной защиты

Организационное и техническое обеспечение процессов генерации, использования, смены и прекращения действия паролей во всех информационных системах предприятия возлагается на работников СИТ.

Для ограничения доступа к ИР, ИС и ОИС предприятия используется защита вида логин-пароль.

Логин пользователю выдается в виде i.ivanov, в латинской транскрипции, где i-первая буква имени, ivanov-фамилия пользователя.

Пароли учетных записей сотрудников изменяются не реже чем раз в 6 месяцев. По истечении срока действия пользователь меняет пароль самостоятельно.

Пароли учетных записей работников СИТ изменяются не реже чем раз в 3 месяца.

Изначальные пароли доступа к программным и аппаратным средствам меняются на соответствующие нижеуказанным критериям.

Все пароли системных учетных записей, а также пароли приложений и активного оборудования, хранятся в базе данных, доступ к которой защищен дополнительным паролем.

Пароль учетной записи пользователя, имеющего дополнительные административные функции, должен быть уникален по отношению к другим паролям учетных записей данного пользователя.

Пароли должны состоять минимум из 8 символов и содержать обязательно минимум одну заглавную букву и цифру, для усиления следует обязательно использовать спецсимволы (латинские буквы различного регистра (a–z, A–Z), цифры (0–9), спецсимволы (^?!@#$%&\*()– \_+=~`[]{}|\:;”\*’/<>).

Пользователи могут выбрать любой вариант пароля, соответствующий описанным выше параметрам.

Контроль соблюдения правил генерации и смены паролей пользователями на рабочих местах осуществляется в автоматическом режиме и средствами доменных политик (оповещение, блокировка, проверка паролей на соответствие критериям).

Новый пароль должен отличаться от предыдущих (доменная политика проверяет на совпадение с предыдущими тремя паролями и запрещает ввод пароля при совпадении).

При смене пароля новое значение должно отличаться от предыдущего не менее чем в 2-х позициях, либо символах. Запрещено генерировать новый пароль путем добавления (замены) одной цифры или символа к старому паролю.

Пользователи предприятия обязаны:

* в случае подозрения на то, что пароль может быть кому–либо известен, сообщить данную информацию СИТ и сменить пароль самостоятельно;

Пользователям запрещается небрежно относиться к конфиденциальности собственных идентификационных реквизитов (в частности, паролей и прочих кодов авторизованного доступа) – это может привести к использованию тех или иных ресурсов третьими лицами от имени данного пользователя (с сокрытием, таким образом, истинного источника действий).

Пользователям запрещено:

* сообщать личные пароли кому–либо;
* передавать пароли кому-либо при помощи почтовых сообщений, а также через различные чаты и мессенджеры, либо любым другим открытым способом через сеть Интернет;
* хранить пароли, записанные на бумаге, в легкодоступном месте;
* использовать один и тот же пароль для доступа к различным информационным системам и ресурсам;
* вывешивать данные об именах пользователей и их паролях на всеобщее обозрение.

Пароли для доступа к ОИС (доменные учетные записи пользователей) хранятся в зашифрованном виде и не могут быть использованы никем, кроме владельцев данных паролей.

За хранение паролей к ОИС (сетевое оборудование и прочие сервисные учетные записи, необходимые для работы с ИС) отвечает администратор системный. В случае отсутствия данного работника, за данную функцию отвечает начальник СИТ.

Работник, ответственный за хранение паролей, обязан:

* обеспечить централизованное хранение паролей;
* организовать резервное копирование баз с паролями не реже 1 раза в неделю;
* обеспечить внеплановую смену пароля пользователя при обращении в СИТ, если пользователь не может это сделать самостоятельно в ближайшее время по независящим от него причинам (отпуск, командировка и т.д.).

Внеплановая полная смена паролей доступа к активам и средствам управления доступом производится в случае прекращения полномочий (увольнение, переход, смена области деятельности и другие обстоятельства) работников СИТ, имеющих доступ к указанным паролям или которым были предоставлены полномочия по управлению парольной защитой информационных систем, ресурсов и ОИС.

В случае увольнения пользователя его учетные записи блокируются работниками СИТ, либо изменяются пароли доступа к ним. По прошествии времени указанные учётные записи могут быть удалены.

Все действия, выполненные другим человеком под вашим паролем, в случае случайного\ целенаправленного раскрытия вашего пароля будут считаться совершенными вами.

# **Приложение 9**

Порядок функционирования шлюза информационной безопасности (межсетевого экрана)

1. Межсетевой экран используется на предприятии с целью:
* защиты сетевых подключений всех компонентов информационной сети предприятия к внешним сетям передачи данных, в том числе сетью Интернет от внешних угроз ИБ;
* предотвращения доступа к небезопасным файлам и сайтам, нецелевого использования сети Интернет;
* обеспечения защищенного доступа к информационной сети предприятия удаленных пользователей БГЦА;
* контроля доступа пользователей к ресурсам сети Интернет с целью определения нецелевого использования;
* журналирования доступа пользователей для формирования отчетности с целью дальнейшего анализа и использования.
1. Настройкой межсетевого экрана занимается СИТ.
2. Идентификация пользователей выполняется с помощью доменных учетных записей и IP-адресов.
3. Аутентификация пользователей выполняется с помощью доменных учетных записей.
4. Регламент работы удаленных пользователей:
	* Авторизация удаленных пользователей для получения доступа выполняется с помощью доменных учетных записей и предустановленного SSL-сертификата.
	* Подключение удаленных пользователей (рабочих мест) и приложений через средства доступа удаленных пользователей осуществляется при помощи межсетевого экрана с использованием специального ПО к межсетевому экрану и организации защищенного VPN соединения.
	* При удаленном подключении используется как парольная защита, так и идентификация удаленных ПК по наличию предустановленного SSL-сертификата.
	* В случае «неактивности»происходит разрыв сеанса удаленного доступа пользователя через 8 часов.
	* Каждый удаленный пользователь может установить только одну сессию для подключения к ИС «БГЦА» и ее объектам (ОИС).
	* Лимит количества неудачных попыток подключения ограничен лимитом попыток ввода учётной записи в домене (5 попыток), после чего указанная учетная запись блокируется. Разблокировать учетную запись может только работник СИТ.

# **Приложение 10**

Организация доступа и резервного копирования информации

1. Резервное копирование информации выполняется с целью обеспечения подлинности, целостности и сохранности информации в электронном виде.
2. Резервное копирование выполняется работниками СИТ, в должностные обязанности которых входит выполнение указанных операций, либо работниками, их заменяющими.
3. Резервное копирование подразделяется на автоматическое (онлайн) и ручное (офлайн).
4. Офлайн копирование выполняется на внешний носитель информации не реже 1-го раза в месяц.
5. Резервные ОИС и носители информации, на которых хранятся резервные копии размещаются на удалении от места расположения основных средств, во избежание их повреждения в случае аварии либо пожара на основном месте размещения средств.
6. Величина допустимой потери данных (RPO) допустимое время восстановления данных (RTO) – не более одного рабочего дня.
	1. Регламент и периодичность резервного копирования баз данных:
		1. Онлайн резервное копирование. Проводится в автоматическом режиме по заранее составленному расписанию. Хранение – на сетевом накопителе NAS.
		2. Базы данных:
* SMBusiness: ежедневно, срок хранения ежедневных копий – 2 недели;
* 1С: ежедневно, срок хранения ежедневных копий – 2 недели;
* ИС «Аккредитация»: ежедневно.
	+ 1. ИР BSCA: по схеме «последние день/неделя/месяц/год» (ежедневные копии за последние 7 дней, 3 копии за последние 3 недели, 6 копий за последние 6 мес. и одна за предыдущий год).
		2. Виртуальные и физические сервера: ежедневно, минимум 10 дней.
	1. Оффлайн резервное копирование: не менее 1 раза в месяц (хранится только одна копия), на внешний жесткий диск.
	2. Резервное копирование по мере необходимости.
	3. Сетевое оборудование. Вручную, после изменения настроек. Резервные копии хранятся на компьютере администратора системного и на сетевом накопителе.

# **Приложение 11**

Регламент доступа к администрированию ОИС

 Физический доступ представителей сторонних организаций, с которыми заключены договора на сопровождение и обслуживание ЛВС и СВТ, в помещения, а также к шкафам с СВТ, сетевым и другим оборудованием осуществляется только ввиду служебной необходимости и допускается только в сопровождении сотрудника СИТ.

 Сотрудникам сторонних организаций, с которыми заключены договора на сопровождения информационных систем, для проведения работ предоставляются специально организованные автоматизированные рабочие места с минимально необходимыми правами и уровнем доступа и только в присутствии сотрудника СИТ. В случае необходимости предоставляется временная учетная запись с ограниченными правами.

 При проведении работ запрещается подключение дополнительного оборудования к ПК, периферийных устройств к ЛВС и съемных машинных носителей информации.

 В случае необходимости использования записанной на съемных машинных носителях информации, сотрудником СИТ предварительно проводятся работы по ее копированию на специально выделенные для этих целей носители информации.

 Не допускается предоставление удаленного доступа к программным и программно-аппаратным средствам, в том числе средствам защиты информации, для обновления или управления со стороны лиц, не являющихся штатным работниками организации, а также работниками его дочерних или подчинённых организаций.