Утверждаю:

Главный врач ООО КЭМ «Антуриум»

_____ Н.В. Татаринцева

«_30_» _1_ _____2022 года

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ООО КЭМ «АНТУРИУМ»

1. Оглавление

2. Введение

Политика информационной безопасности (далее – Политика) Общества с ограниченной ответственностью Клиника Эстетической Медицины «Антуриум» (далее – ООО КЭМ «Антуриум») определяет систему взглядов на проблему обеспечения информационной (далее – ИБ). Представляет собой систематизированное изложение высокоуровневых целей и задач защиты, которыми необходимо руководствоваться в своей деятельности, а также основных принципов построения системы управления информационной безопасностью (далее – СУИБ) ООО КЭМ «Антуриум».

Обеспечение информационной безопасности – необходимое условие для успешного осуществления уставной деятельности Учреждения.

Обеспечение информационной безопасности включает в себя любую деятельность, направленную на защиту информационных ресурсов и/или поддерживающей инфраструктуры. Политика охватывает все автоматизированные и телекоммуникационные системы, владельцем и пользователем которых является ООО КЭМ «Антуриум».

Реализация Политики должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информационных ресурсов не только с помощью отдельного средства, но и с помощью их простой совокупности. Необходимо их системное, согласованное между собой применение, а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой информационной системы в защищенном исполнении при оптимальном соотношении технических и организационных мероприятий.

3. Обозначения и сокращения

АРМ	Автоматизированное рабочее место
АС	Автоматизированная система
ГБУ	Государственное бюджетное учреждение
ИБ	Информационная безопасность
ИР	Информационный ресурс
ИС	Информационная система
ИС СМТ	Информатизации и связи спутникового мониторинга транспорта
ИТ	Информационные технологии
НСД	Несанкционированный доступ
ОКЗ	Орган криптографической защиты
ПО	Программное обеспечение
СКЗИ	Средство криптографической защиты информации
СУИБ	Система управления информационной безопасностью

4. Термины и определения

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Авторизация – предоставление субъекту прав на доступ, а также предоставление доступа в соответствии с установленными правами на доступ.

Аутентификация – проверка принадлежности субъекту доступа предъявленного им идентификатора; подтверждение подлинности.

Безопасность информации – защищенность информации от ее нежелательного разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности, а также незаконного ее тиражирования.

Бизнес-процесс – последовательность технологически связанных операций по предоставлению продуктов, услуг и/или осуществлению конкретного вида деятельности Учреждения.

Владелец актива – физическое или юридическое лицо, которое наделено административной ответственностью за руководство изготовлением, разработкой, хранением, использованием и безопасностью актива. Термин «владелец» не означает, что этот человек фактически имеет право собственности на этот актив.

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах, установленных законом.

Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Доступность информации – состояние, характеризуемое способностью ИС обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию и средства доступа к ней.

Идентификация – присвоение субъектам доступа, объектам доступа идентификаторов (уникальных имен) и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Информационная безопасность (ИБ) – состояние защищенности интересов Учреждения.

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Информационный процесс – процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

Информационный ресурс (актив) – все, что имеет ценность и находится в распоряжении Учреждения.

Инцидент – непредвиденное или нежелательное событие (группа событий) безопасности, которое привело (могут привести) к нарушению функционирования информационной системы или возникновению угроз безопасности информации (нарушению конфиденциальности, целостности, доступности).

Инцидент информационной безопасности – одно или серия нежелательных или неожиданных событий ИБ, имеющих значительную вероятность нарушения бизнес-процессов или представляющих угрозу ИБ.

Коммерческая тайна – конфиденциальность информации, позволяющая ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду.

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств.
Конфиденциальная информация – информация с ограниченным доступом, не содержащая сведений, составляющих государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.
Конфиденциальность информации – состояние защищенности информации, характеризуемое способностью ИС обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней.
Мобильный код – несамостоятельное программное обеспечение или компонент программного обеспечения (скрипты, макросы, иные компоненты) получаемые из мест распространения мобильного кода, передаваемые по сети и выполняемые на компонентах информационной системы (в местах использования мобильного кода) без предварительной установки (инсталляции) пользователем для расширения возможностей системного и (или) прикладного программного обеспечения.
Несанкционированный доступ – доступ к информации иди действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.
Обработка риска – процесс выбора и реализации мер по модификации (снижению) риска.
Политика – общие цели и указания, формально выраженные руководством.
Привилегии – это права доверенного объекта на совершение каких-либо действий по отношению к объектам системы.
Риск – сочетание вероятности события и его последствий.
Система управления информационной безопасностью (СУИБ) – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования ИБ.
Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, в полном объеме реализующий полномочия владения, пользования, распоряжения указанными объектами.
События информационной безопасности – идентифицированное состояние системы, сервиса или сети, свидетельствующее о возможном нарушении политики безопасности или отсутствии механизмов защиты, либо прежде неизвестная ситуация, которая может иметь отношение к безопасности.
Угроза – Опасность, предполагающая возможность потерь (ущерба).
Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.

5. Цель

Основной целью, на достижение которой направлены все положения настоящей Политики, является защита информационных ресурсов от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители, процессы обработки и передачи, а также минимизация рисков ИБ.
Для достижения основной цели необходимо обеспечивать эффективное решение следующих задач:

- своевременное выявление, оценка и прогнозирование источников угроз ИБ;
- создание механизма оперативного реагирования на угрозы ИБ;
- предотвращение и/или снижение ущерба от реализации угроз ИБ;
- защита от вмешательства в процесс функционирования ИС посторонних лиц;

соответствие требованиям Федерального законодательства, нормативно-методических документов ФСБ России, ФСТЭК России и договорным обязательствам в части ИБ;
обеспечение непрерывности критических бизнес-процессов;
достижение адекватности мер по защите от угроз ИБ;
изучение партнеров, клиентов, конкурентов и кандидатов на работу;
недопущение проникновения структур организованной преступности и отдельных лиц с противоправными намерениями;
выявление, предупреждение и пресечение возможной противоправной и иной негативной деятельности сотрудников;
повышение деловой репутации и корпоративной культуры.

6. Основания для разработки

Настоящая политика разработана на основе требований законодательства Российской Федерации, накопленного в ООО КЭМ «Антуриум» опыта в области обеспечения ИБ, интересов и целей ООО КЭМ «Антуриум».
При написании отдельных положений настоящей политики использовались следующие нормативные документы:

ГОСТ Р ИСО/МЭК 27001 «Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности»;
РС БР ИББС-2.0-2007 «Методические рекомендации по документации в области обеспечения информационной безопасности…»;
РС БР ИББС-2.2-2009 «Методика оценки рисков нарушения информационной безопасности»;
РС БР ИББС-2.5-2014 «Менеджмент инцидентов информационной безопасности»;
СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы РФ. Общие положения».

7. Область действия

Настоящая Политика распространяется на все бизнес-процессы ООО КЭМ «Антуриум» и обязательна для применения всеми сотрудниками и руководством ООО КЭМ «Антуриум», а также пользователями его информационных ресурсов.
Настоящая политика распространяется на информационные системы ООО КЭМ «Антуриум».
Лица, осуществляющие разработку внутренних документов ООО КЭМ «Антуриум», регламентирующих вопросы информационной безопасности, обязаны руководствоваться настоящей Политикой.

8. Содержание политики

8.1. Система управления информационной безопасностью

Для достижения указанных целей и задач в Учреждении внедряется система управления информационной безопасностью.

СУИБ документирована в настоящей политике, в правилах, процедурах, рабочих инструкциях, которые являются обязательными для всех работников ООО КЭМ «Антуриум» в области действия системы. Документированные требования СУИБ доводятся до сведения работников ООО КЭМ «Антуриум».
Средства управления информационной безопасностью внедряются по результатам проведения оценки рисков информационной безопасности.
Стоимость внедряемых средств управления информационной безопасностью не должна превышать возможный ущерб, возникающий при реализации угроз.

8.1.1. Структура документов

В целях создания взаимосвязанной структуры нормативных документов ООО КЭМ «Антуриум» в области обеспечения информационной безопасности, разрабатываемые и обновляемые нормативные документы должны соответствовать следующей иерархии:

Настоящая Политика является внутренним нормативным документом по ИБ первого уровня.

Документы второго уровня – инструкции, порядки, регламенты и прочие документы, описывающие действия сотрудников Учреждения по реализации документов первого и второго уровня.

Документы третьего уровня – отчетные документы о выполнении требований документов верхних уровней.

8.1.2. Ответственность за обеспечение ИБ

Для непосредственной организации и эффективного функционирования системы обеспечения информационной безопасности в Учреждении функции обеспечения ИБ возложены на ответственного за обеспечение безопасности, и на него возлагается решение следующих основных задач:

проведение в жизнь Политики ИБ;

определение требований к защите информации;

организация мероприятий и координация работ всех подразделений по вопросам комплексной защиты информации;

контроль и оценка эффективности принятых мер и применяемых средств защиты;

оказание методической помощи сотрудникам в вопросах обеспечения информационной безопасности;

регулярная оценка и управление рисками информационной безопасности в соответствии с установленными процедурами в области управления рисками;

выбор и внедрение средств защиты информации, включая организационные, физические, технические, программные и программно-аппаратные средства обеспечения СУИБ;

обеспечение минимально-необходимого доступа к информационным ресурсам, основываясь на требованиях бизнес-процессов;

информирование, обучение и повышение квалификации работников ООО ММК «Антуриум» в сфере информационной безопасности;

расследования инцидентов информационной безопасности;

сбор, накопление, систематизация и обработка информации по вопросам информационной безопасности;

обеспечение необходимого уровня отказоустойчивости ИТ-сервисов и доступности данных для подразделений.

Для решения задач ответственный за обеспечение безопасности имеет следующие права:

определять необходимость и разрабатывать нормативные документы, касающиеся вопросов обеспечения безопасности информации, включая документы, регламентирующие деятельность пользователей информационной системы в указанной области;
получать информацию от пользователей информационных систем ООО КЭМ «Антуриум» по любым аспектам применения информационных технологий в ООО КЭМ «Антуриум»;
участвовать в проработке технических решений по вопросам обеспечения безопасности информации при проектировании и разработке новых информационных технологий;
участвовать в испытаниях разработанных информационных технологий по вопросам оценки качества реализации требований по обеспечению безопасности информации;
контролировать деятельность пользователей по вопросам обеспечения ИБ;
готовить предложения руководству по обеспечению требований ИБ.

8.2. Объект защиты

8.2.1. Ответственность за ресурсы

В ООО КЭМ «Антуриум» должны быть выявлены и оценены с точки зрения их важности все ресурсы. Для всех ценных ресурсов должен быть составлен реестр (перечень). Благодаря информации о ресурсах ООО КЭМ «Антуриум» реализуется защита информации, степень которой соразмерна ценности и важности ресурсов.
В ИС ООО КЭМ «Антуриум» присутствуют следующие типы ресурсов:

информационные ресурсы, содержащие конфиденциальную информацию, и/или сведения ограниченного доступа, в том числе информацию о финансовой деятельности ООО КЭМ «Антуриум»;
открыто распространяемая информация, необходимая для работы ООО КЭМ «Антуриум», независимо от формы и вида ее представления;
информационная инфраструктура, включая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы.

Для каждого ресурса должен быть назначен владелец, который отвечает за соответствующую классификацию информации и ресурсов, связанных со средствами обработки информации, а также за назначение и периодическую проверку прав доступа и категорий, определенных политиками управления доступа.

8.2.2. Классификация информации

Все информационные ресурсы, подлежащие защите, должны быть классифицированы в соответствии с важностью и степенью доступа. Классификация информации должна быть документирована и утверждена руководством ООО КЭМ «Антуриум».
Классификация информации должна проводиться владельцем ресурса, хранящего или обрабатывающего информацию, для определения категории ресурса. Периодически классификация должна пересматриваться для поддержания актуальности ее соответствия с категорией ресурса.
Ресурсы, содержащие конфиденциальную или критичную информацию, должны иметь соответствующую пометку (гриф).

8.3. Оценка и обработка рисков

В ООО КЭМ «Антуриум» должны быть определены требования к безопасности путем методической оценки рисков. Оценки рисков должны выявить, определить количество и расположить по приоритетам риски в соответствии с критериями принятия рисков и бизнес-целями учреждения. Результаты оценки должны определять соответствующую реакцию руководства, приоритеты управления рисками ИБ и набор механизмов контроля для защиты от этих рисков.

Оценка рисков предполагает системное сочетание анализа рисков и оценивания рисков.

Кроме того, оценка рисков и выбор механизмов контроля должны производиться периодически, чтобы:

- учесть изменения бизнес-требований и приоритетов;
- принять во внимание новые угрозы и уязвимости;
- убедиться в том, что реализованные средства сохранили свою эффективность.

Перед обработкой каждого риска ООО КЭМ «Антуриум» должно выбрать критерии для определения возможности принятия этого риска. Риск может быть принят, если его величина достаточно мала и стоимость обработки нерентабельна для ООО КЭМ «Антуриум». Такие решения должны регистрироваться.

Для каждого из оцененных рисков должно приниматься одно из решений по его обработке:

- применение соответствующих механизмов контроля для уменьшения величины риска до приемлемого уровня;
- сознательное и объективное принятие риска, если он точно удовлетворяет Политике ООО КЭМ «Антуриум» и критериям принятия рисков;
- уклонение от риска путем недопущения действий, могущих быть его причиной;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

8.4. Безопасность персонала

Роли и обязанности по обеспечению безопасности информационных ресурсов, описанные в соответствии с Политикой ИБ ООО КЭМ «Антуриум», должны быть доведены до сотрудника при трудоустройстве и внесены в его должностные обязанности. Сюда должны входить как общие обязанности по реализации и поддержке политики безопасности, так и конкретные обязанности по защите ресурсов и по выполнению конкретных операций, связанных с безопасностью.

8.4.1. Условия найма

Все принимаемые на работу сотрудники должны одобрить и подписать свои трудовые договоры, в которых устанавливается их ответственность за ИБ. В договор должно быть включено согласие сотрудника на проведение контрольных мероприятий со стороны ООО КЭМ «Антуриум» по проверке выполнения требований ИБ, а также обязательства по неразглашению конфиденциальной информации. В договоре должны быть описаны меры, которые будут приняты в случае несоблюдения сотрудником требований ИБ.

Обязанности по обеспечению ИБ должны быть включены в должностные инструкции каждого сотрудника ООО КЭМ «Антуриум».

Все принимаемые сотрудники должны быть ознакомлены под роспись с перечнем информации, ограниченного доступа, с установленным режимом с ней и с мерами ответственности за нарушение этого режима.

При предоставлении сотруднику доступа к ИС ООО КЭМ«Антуриум» он должен ознакомиться под роспись с инструкцией пользователя ИС.

8.4.2. Ответственность руководства

Руководство ООО КЭМ «Антуриум» должно требовать от всех сотрудников, подрядчиков и пользователей сторонних организаций принятия мер безопасности в соответствии с установленными в ООО КЭМ «Антуриум» политиками и процедурами.

Уполномоченные руководством ООО КЭМ «Антуриум» сотрудники имеют право в установленном порядке, без уведомления пользователей, производить проверки:

- Выполнения действующих инструкций по вопросам ИБ;
- Данных, находящихся на носителях информации;
- Порядка использования сотрудниками информационных ресурсов;
- Содержания служебной переписки.

8.4.3. Обучение ИБ

Все сотрудники должны проходить периодическую подготовку в области политики и процедур ИБ, принятых в ООО КЭМ «Антуриум».

8.4.4. Завершение или изменения трудовых отношений

При увольнении все предоставленные сотруднику права доступа к ресурсам ИС должны быть удалены. При изменении трудовых отношений удаляются только те права, необходимость в которых отсутствует в новых отношениях.

8.5. Физическая безопасность

8.5.1. Защищенные области

Средства обработки информации, поддерживающие критически важные и уязвимые ресурсы ООО КЭМ «Антуриум», должны быть размещены в защищенных областях. Такими средствами являются: серверы, магистральное телекоммуникационное оборудование, телефонные станции, кроссовые панели, оборудование, обеспечивающее обработку и хранение конфиденциальной информации.

Защищенные области должны обеспечиваться соответствующими средствами контроля доступа, обеспечивающим возможность доступа только авторизованного персонала.

Запрещается прием посетителей в помещениях, когда осуществляется обработка информации ограниченного доступа.

Для хранения служебных документов и машинных носителей с защищаемой информацией помещения снабжаются сейфами, металлическими шкафами или шкафами, оборудованными замком.

Помещения должны быть обеспечены средствами уничтожения документов.

8.5.2. Области общего доступа

Места доступа, через которые неавторизованные лица могут попасть в помещения ООО КЭМ «Антуриум», должны контролироваться и, если это возможно, должны быть изолированы от средств обработки информации с целью предотвращения несанкционированного доступа.

8.5.3. Вспомогательные службы

Все вспомогательные службы, такие как электропитание, водоснабжение, канализация, отопление, вентиляция и кондиционирование воздуха должны обеспечивать гарантированную и устойчивую работоспособность компонентов ИС ООО КЭМ «Антуриум».

8.5.4. Утилизация или повторное использование оборудования

Со всех носителей информации, которыми укомплектовано утилизируемое оборудование, должны гарантированно удаляться все конфиденциальные данные и лицензионное ПО. Отсутствие защищаемой информации на носителях должно быть проверено ответственным за обеспечение безопасности, о чем должна быть сделана отметка в акте списания.

8.5.5. Перемещение имущества

Оборудование, информация или ПО должны перемещаться за пределы ООО КЭМ «Антуриум» только при наличии письменного разрешения руководства. Сотрудники, имеющие право перемещать оборудование и носители информации за пределы ООО КЭМ «Антуриум» должны быть четко определены. Время перемещения оборудования за пределы ООО КЭМ «Антуриум» и время его возврата должны регистрироваться.

8.6. Контроль доступа

Основными пользователями информации в информационной системе ООО КЭМ «Антуриум» являются сотрудники структурных подразделений. Уровень полномочий каждого пользователя определяется индивидуально. Каждый сотрудник пользуется только предписанными ему правами по отношению к информации, с которой ему необходимо работать в соответствии с должностными обязанностями.

Допуск пользователей к работе с информационными ресурсами должен быть строго регламентирован. Любые изменения состава и полномочий пользователей подсистем должны производиться в установленном порядке, согласно «перечню лиц, имеющим право доступа к ИС», а так же «матрице доступа».

Каждому пользователю, допущенному к работе с конкретным информационным активом ООО КЭМ «Антуриум», должно быть сопоставлено персональное уникальное имя (учетная запись пользователя), под которым он будет регистрироваться и работать с ИС.

В случае производственной необходимости некоторым сотрудникам могут быть сопоставлены несколько уникальных имен (учетных записей).

Временная учетная запись может быть заведена для пользователя на ограниченный срок для выполнения задач, требующих расширенных полномочий, или для проведения настройки, тестирования информационной системы, для организации гостевого доступа (посетителям, сотрудникам сторонних организаций, стажерам и иным пользователям с временным доступом к информационной системе).

В общем случае запрещено создавать и использовать общую пользовательскую учетную запись для группы пользователей. В случаях, когда это необходимо, ввиду особенностей автоматизируемого бизнес-процесса или организации труда (например, посменное дежурство), использование общей учетной записи должно сопровождаться отметкой в журнале учета машинного времени, которая должна однозначно идентифицировать текущего владельца учетной записи в каждый момент времени. Одновременное использование одной общей пользовательской учетной записи разными пользователями запрещено.

Регистрируемые учетные записи подразделяются на:

Пользовательские – предназначенные для аутентификации пользователей ИС ООО КЭМ «Антуриум»;

Системные – используемые для нужд операционной системы;

Служебные – предназначенные для функционирования отдельных процессов или приложений.

Системные учетные записи формируются операционной системой и должны использоваться только в случаях, предписанных документацией на операционную систему.

Служебные учетные записи используются только для запуска и работы сервисов или приложений.

Использование системных или служебных учетных записей для регистрации пользователей в системе категорически запрещено.

Процедуры регистрации и блокирования учетных записей пользователей должны применяться с соблюдением следующих правил:

использование уникальных идентификаторов (ID) пользователей для однозначного определения и сопоставления личности с совершенными ей действиями;

использование групповых ID разрешать только в случае, если это необходимо для выполнения задачи;

предоставление и блокирование прав должны быть санкционированы и документированы;

предоставление прав доступа к ИР, только после согласования с владельцем данного ИР;

регистрация и блокирование учетных записей допускается с отдельного разрешения руководства ООО КЭМ «Антуриум»;

уровень предоставленных полномочий должен соответствовать производственной необходимости и настоящей Политике и не ставить под угрозу разграничение режимов работы;

согласование изменения прав доступа с ответственным за обеспечение безопасности;

документальная фиксация назначенных пользователю прав доступа;

ознакомление пользователей под подпись с письменными документами, в которых регламентируются их права доступа;

предоставление доступа с момента завершения процедуры регистрации;

обеспечение создания и поддержания формального списка всех пользователей, зарегистрированных для работы с ИР или сервисом;

немедленное удаление или блокирование прав доступа пользователей, сменивших должность, форму занятости или уволившихся из ООО КЭМ «Антуриум»;

аудит ID и учетных записей пользователей на наличие неиспользуемых, их удаление и блокировка;

обеспечение того, чтобы лишние ID пользователей не были доступны другим пользователям;

обеспечить возможность предоставления пользователям доступа в соответствии с их должностями, основанными на производственных требованиях, путем суммирования некоторого числа прав доступа в типовые профили доступа пользователей.

8.6.1. Управление привилегиями

Доступ сотрудника к информационным ресурсам ООО КЭМ «Антуриум» должен быть санкционирован руководителем структурного подразделения, в котором числится согласно штатному расписанию данный сотрудник, и владельцами соответствующих информационных ресурсов. Управление доступом осуществляется в соответствии с установленными процедурами.

Наделение привилегиями и их использование должно быть строго ограниченным и управляемым. Распределение привилегий должно управляться с помощью процесса регистрации этих привилегий. Должны быть рассмотрены следующие этапы:

должны быть идентифицированы привилегии доступа, связанные с каждым системным продуктом, например, с операционной системой, системой управления базой данных и каждым приложением, а также пользователи, которым они должны быть предоставлены;

привилегии должны предоставляться пользователям на основании «производственной необходимости» и только на период времени, необходимый для достижения поставленных целей, например, привилегии, минимально необходимые для выполнения их функциональных обязанностей, только тогда, когда эти привилегии необходимы;

должен быть обеспечен процесс санкционирования всех предоставленных привилегий и создание отчетов по ним, привилегии нельзя предоставлять до завершения процесса их регистрации;

уникальные привилегии должны присваиваться на другой ID пользователя, не тот, который используется при обычной работе пользователя.

Контроль и периодический пересмотр прав доступа пользователей к информационным ресурсам ООО КЭМ «Антуриум» осуществляется в процессе аудита ИБ в соответствии с Правилами аудита ИБ и установленными процедурами.

8.6.2. Управление паролями

Пароли – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю.

Предоставление паролей должно контролироваться посредством официальной процедуры, отвечающей следующим требованиям:

все пользователи должны быть ознакомлены под роспись с требованием сохранения в тайне личных и групповых паролей;

при наличии возможности, необходимо настроить систему таким образом, чтобы при первом входе пользователя с назначенным ему временным паролем система сразу же требовала его сменить;

временные пароли должны назначаться пользователю только после его идентификации;

необходимо избегать передачи паролей с использованием третьих лиц или незашифрованной электронной почтой;

временные пароли не должны быть угадываемыми и повторяющимися от пользователя к пользователю;

пользователь должен подтвердить получение пароля;

пароли должны храниться в электронном виде только в защищенной форме;

назначенные производителем ПО пароли должны быть изменены сразу после завершения инсталляции;

необходимо установить требования к длине пароля, набору символов и числу попыток ввода;

необходимо изменять пароля пользователя не реже одного раза в 90 дней.

При необходимости можно рассмотреть возможность использования других технологий идентификации и аутентификации пользователей, в частности, биометрических технологий, проверки подписи и аппаратных средств (смарт-карты, e-Token/ruToken, чипы и т.п.).

8.6.3. Контроль прав доступа

Чтобы обеспечить эффективный контроль доступа необходимо ввести официальный процесс регулярной проверки прав доступа пользователей, отвечающий следующим требованиям:

права доступа пользователей должны проверяться через регулярные интервалы (не реже одного раза в полгода), а также после внесения каких-либо изменений в ИС;

права доступа пользователей должны проверяться и переназначаться при изменении их должностных обязанностей в Учреждении, а также при переходе с одной работы на другую в пределах Учреждения;

проверка прав пользователей, имеющих особые привилегии для доступа в систему, должна проводиться чаще (не реже одного раза в 3 месяца);

необходимо регулярно проверять адекватность назначенных привилегий, во избежание получения кем-либо из пользователей излишних прав;

изменение привилегированных учетных записей должно протоколироваться.

Контроль над выполнением процедур управления доступом пользователей должен включать:

контроль над добавлением, удалением и изменением идентификаторов, аутентификационных данных и иных объектов идентификации;

проверку подлинности пользователей перед сменой паролей;

немедленное блокирование прав доступа при увольнении;

блокирование учетных записей, неактивных более 45 дней;

включение учетных записей, используемых поставщиками для удаленной поддержки, только на время выполнения работ;

отслеживание удаленных учетных записей, используемых поставщиками, во время работ;

предотвращение повторного использования идентификатора пользователя и (или) устройства в течение не менее трех лет;

ознакомление с правилами и процедурами аутентификации всех пользователей, имеющих доступ к сведениям ограниченного распространения;

использование механизмов аутентификации при доступе к любой базе данных, содержащей сведения ограниченного распространения, в том числе доступе со стороны приложений, администраторов и любых других пользователей;

разрешение запросов и прямого доступа к базам данных только для администраторов баз данных;

блокирование учетной записи на период равный 30 минутам или до разблокировки учетной записи администратором;

блокирование учетных записей пользователей при выявлении по результатам мониторинга (просмотра, анализа) журналов регистрации событий безопасности действий пользователей, которые отнесены оператором к событиям нарушения безопасности информации.

8.6.4. Использование паролей

Идентификатор и пароль пользователя в ИС являются учетными данными, на основании которых сотруднику ООО КЭМ «Антуриум» предоставляются права доступа, протоколируются производимые им в системе действия и обеспечивается режим конфиденциальности, обрабатываемой (создаваемой, передаваемой и хранимой) сотрудником информации.

Не допускается использование различными пользователями одних и тех же учетных данных.

Первоначальное значение пароля учетной записи пользователя устанавливает ответственный за обеспечение безопасности ПДн.

Личные пароли устанавливаются первый раз ответственным за обеспечение безопасности ИС в ООО КЭМ «Антуриум». После первого входа в систему и в дальнейшем пароли выбираются пользователями автоматизированной системы самостоятельно с учетом следующих требований:

длина пароля должна быть не менее 8 символов;

в числе символов пароля должны присутствовать три из четырех видов символов:

буквы в верхнем регистре;

буквы в нижнем регистре;

цифры;

специальные символы (! @ # $ % ^ & * ( ) — _ + = ~ [ ] { } | \ : ; ‘ » < > , . ? /);

пароль не должен содержать легко вычисляемые сочетания символов, например,

имена, фамилии, номера телефонов, даты;

последовательно расположенные на клавиатуре символы («12345678», «QWERTY», и т.д.);

общепринятые сокращения («USER», «TEST» и т.п.);

повседневно используемое слово, например, имена или фамилии друзей, коллег, актеров или сказочных персонажей, клички животных;

компьютерный термин, команда, наименование компаний, web сайтов, аппаратного или программного обеспечения;

что-либо из вышеперечисленного в обратном написании;

что-либо из вышеперечисленного с добавлением цифр в начале или конце;

при смене пароля значение нового должно отличаться от предыдущего не менее чем в 4 позициях;

для различных ИС необходимо устанавливать собственные, отличающиеся пароли.

Сотруднику запрещается:

сообщать свой пароль кому-либо;

указывать пароль в сообщениях электронной почты;

хранить пароли, записанные на бумаге, в легко доступном месте;

использовать тот же самый пароль, что и для других систем (например, домашний интернет провайдер, бесплатная электронная почта, форумы и т.п.);

использовать один и тот же пароль для доступа к различным корпоративным ИС.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

Сотрудник обязан:

в случае подозрения на то, что пароль стал кому-либо известен, поменять пароль и сообщить о факте компрометации ответственному за обеспечение безопасности и ответственному за организацию обработки ПДн;

немедленно сообщить ответственному за обеспечение безопасности и ответственному за организацию обработки ПДн в случае получения от кого-либо просьбы сообщить пароль;

менять пароль каждые 90 дней;

менять пароль по требованию ответственного за обеспечение безопасности.

После 20 неудачных попыток ввода пароля учетная запись блокируется на 10 минут. При систематической блокировке учетной записи работником (более 3 раз) оповещается ответственный за обеспечение безопасности.

ООО КЭМ «Антуриум» оставляет за собой право:

осуществлять периодическую проверку стойкости паролей пользователей, используемых сотрудниками для доступа к ИС;

принимать меры дисциплинарного характера к сотрудникам, нарушающим положения настоящей политики.

8.6.5. Пользовательское оборудование, оставляемое без присмотра

Пользователи должны обеспечивать необходимую защиту оборудования, остающегося без присмотра. Все пользователи должны быть осведомлены о требованиях ИБ и правилах защиты остающегося без присмотра оборудования, а также о своих обязанностях по обеспечению этой защиты.

8.6.6. Политика чистого стола

Сотрудники ООО КЭМ «Антуриум» обязаны:

сохранять известные им пароли в тайне;

закрывать активные сеансы по завершении работы, если только их нельзя защитить подходящим блокирующим механизмом, например, защищенный паролем хранитель экрана;

по завершении сеанса выходить из системы у универсальных ЭВМ, серверов и офисных ПК.

Запрещается вести запись паролей (например, на бумаге, в программном файле или в карманном устройстве), за исключением случаев, когда запись может храниться безопасно, а метод хранения был утвержден.

Документы и носители с конфиденциальной информацией должны убираться в запираемые места (сейфы, шкафы и т.п.), особенно при уходе с рабочего места.

Компьютеры и терминалы должны быть оставлены в состоянии выполненного выхода из системы, когда они находятся без присмотра.

Вход пользователя в систему не должен выполняться автоматически. Покидая рабочее место пользователь обязан заблокировать компьютер (используя комбинации Win + «L» или Ctrl + Alt + Delete → «Блокировать компьютер»).

Документы, содержащие конфиденциальную информацию, должны изыматься из печатающих устройств немедленно.

В конце рабочего дня сотрудник должен привести в порядок письменный стол и убрать все офисные документы в запираемый шкаф или сейф.

Для утилизации конфиденциальных документов, должны использоваться уничтожители бумаги.

По окончании рабочего дня и в случае длительного отсутствия на рабочем месте необходимо запирать на замок все шкафы и сейфы.

8.6.7. Мобильное компьютерное оборудование

При использовании мобильных средств (например, ноутбуков, планшетов и мобильных телефонов) необходимо соблюдать особые меры предосторожности, чтобы не допустить компрометацию информации, принадлежащей ООО КЭМ «Антуриум». Необходимо принять официальную политику, учитывающую риск, связанный с использованием мобильных компьютеров, и в частности с работой в незащищенной среде.

8.7. Политика допустимого использования информационных ресурсов

Общие обязанности пользователя:

при работе с ПО руководствоваться нормативной документацией (руководством пользователя);

обращаться к ответственному за обеспечение безопасности по всем техническим вопросам, связанным с работой в корпоративной ИС (подключение к корпоративной ИС/домену, инсталляция и настройка ПО, удаление вирусов, предоставление доступа в сеть Интернет и к внутренним сетевым ресурсам, ремонт и техническое обслуживание и т.п.), а также за необходимой методологической/консультационной помощью по вопросам применения технических и программных средств корпоративной ИС;

знать признаки правильного функционирования установленных программных продуктов и средств защиты информации;

минимизировать вывод на печать обрабатываемой информации.

Пользователю запрещено производить несанкционированное распространение справочной информации, которая становится доступна при подключении к корпоративной ИС ООО КЭМ «Антуриум».

8.7.1. Использование ПО

На АРМ ООО ММК «Антуриум» допускается использование только лицензионного программного обеспечения, утвержденного в перечне разрешенного программного обеспечения.

Запрещено незаконное хранение на жестких дисках АРМ ООО КЭМ «Антуриум» информации, являющейся объектом авторского права (ПО, фотографии, музыкальные файлы, игры, и т.д.).

Решение о приобретении и установке программного обеспечения, необходимого для реализации медицинских, финансовых, административно-хозяйственных и других задач принимает главный врач по представлении ответственного за организацию обработки ПДн.

Документы, подтверждающие покупку программного обеспечения, хранятся в бухгалтерии на протяжении всего времени использования лицензии, копии указанных документов вместе с лицензионными соглашениями на ПО, ключами защиты ПО и дистрибутивами хранятся у ответственного за организацию обработки ПДн или ответственного за обеспечение безопасности.

Пользователи АРМ не имеют права удалять, изменять, дополнять, обновлять программную конфигурацию на АРМ ООО КЭМ «Антуриум». Указанные работы, а так же работы по установке, регистрации и активации приобретенного лицензионного ПО могут быть выполнены только ответственным за обеспечение безопасности.

Сведения о вновь приобретенном программном обеспечении должны быть внесены в перечень разрешенного программного обеспечения.

8.7.2. Использование АРМ и ИС

К работе в ИС ООО КЭМ «Антуриум» допускаются лица, назначенные на соответствующую должность и прошедшие инструктаж по вопросам информационной безопасности.

Каждому сотруднику ООО КЭМ «Антуриум», которому необходим доступ к ИР в рамках его должностных обязанностей, выдаются под роспись необходимые средства автоматизации. Ответственность по установке и поддержке всех компьютерных систем, функционирующих в ООО КЭМ «Антуриум», возложена на ответственного за обеспечение безопасности.

Каждый сотрудник ООО КЭМ «Антуриум», обеспеченный АРМ, получает персональное сетевое имя, пароль, адрес электронной почты и личный каталог в сети, который предназначен для хранения рабочих файлов.

Работа в ИС сотрудникам разрешена только на закрепленных за ними АРМ, в определенное время и только с разрешенным программным обеспечением и сетевыми ресурсами.

Все АРМ, установленные в ООО КЭМ «Антуриум», имеют унифицированный набор офисных программ, предназначенных для получения, обработки и обмена информацией, определенный в техническом паспорте ИС ООО КЭМ «Антуриум». Изменение установленной конфигурации возможно после внесения соответствующих поправок в стандарт рабочих мест или по служебной записке, согласованной с ответственным за обеспечение безопасности. Комплектация персональных компьютеров аппаратными и программными средствами, а также расположение компьютеров контролируется ответственным за обеспечение безопасности.

Самостоятельная установка программного обеспечения на АРМ запрещена. Установка и удаление любого программного обеспечения производится только ответственным за обеспечение безопасности.

В случае обнаружения неисправности компьютерного оборудования или программного обеспечения, пользователь должен обратиться к ответственному за обеспечение безопасности.

Ответственный за обеспечение безопасности имеют право осуществлять контроль над установленным на компьютере программным обеспечением, и принимать меры по ограничению возможностей несанкционированной установки программ.

При работе в ИС ООО КЭМ «Антуриум» сотрудник обязан:

- знать и выполнять требования внутренних организационно-распорядительных документов ООО ММК «Антуриум»;
- использовать ИС и АРМ ООО КЭМ «Антуриум» исключительно для выполнения своих служебных обязанностей;
- ставить в известность ответственного за обеспечение безопасности о любых фактах нарушения требований ИБ;
- ставить в известность ответственного за обеспечение безопасности о любых фактах сбоев ПО, некорректного завершения значимых операций, а также повреждения технических средств;
- незамедлительно выполнять предписания ответственного за обеспечение безопасности ООО КЭМ «Антуриум».
- Предоставлять АРМ ответственному за обеспечение безопасности для контроля;
- При необходимости прекращения работы на некоторое время корректно закрывать все активные задачи, блокировать АРМ;
- В случае необходимости продолжения работы по окончании рабочего дня проинформировать об этом ответственного за обеспечение безопасности.

При использовании ИС ООО КЭМ «Антуриум» запрещено:

- использовать АРМ и ИС в личных целях;
- отключать средства управления и средства защиты, установленные на рабочей станции;
- передавать:
  - конфиденциальную информацию за исключением случаев, когда это входит в служебные обязанности и способ передачи является безопасным, согласованным с ответственным за обеспечение безопасности;
  - информацию, файлы или ПО, способные нарушить или ограничить функциональность любых программных и аппаратных средств, а также ссылки на вышеуказанные объекты;
  - угрожающую, клеветническую, непристойную информацию;
- самовольно вносить изменения в конструкцию, конфигурацию, размещение АРМ и других узлов ИС ООО КЭМ «Антуриум»;
- предоставлять сотрудникам ООО КЭМ «Антуриум» (за исключением ответственных лиц) и третьим лицам доступ к своему АРМ;
- запускать на АРМ ПО, не входящее в Реестр разрешенного к использованию ПО;
- защищать информацию, способами, не согласованными с ответственным за обеспечение безопасности заранее;
- самостоятельно подключать рабочую станцию и прочие технические средства к корпоративной ИС ООО КЭМ «Антуриум»;
- осуществлять поиск средств и путей повреждения, уничтожения технических средств и ресурсов ИС или осуществлять попытки несанкционированного доступа к ним;
- использовать для выполнения служебных обязанностей локальные (не доменные) учетные записи АРМ.

Информация о посещаемых ресурсах ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству ООО КЭМ «Антуриум».

Все электронные сообщения и документы в электронном виде, передаваемые посредством ИС ООО КЭМ «Антуриум» подлежат обязательной проверке на отсутствие вредоносного ПО.

8.7.3. Использование ресурсов локальной сети

Для выполнения своих служебных обязанностей каждый сотрудник обеспечивается доступом к соответствующим информационным ресурсам. Информационными ресурсами являются каталоги и файлы, хранящиеся на дисках серверов ООО КЭМ «Антуриум», базы данных, электронная почта.

Основными рабочими каталогами являются базы дынных, личные каталоги сотрудников, созданные в соответствии с особенностями их работы. Доступ сотрудников к ресурсам сети осуществляется согласно матрице доступа. Временное расширение прав доступа осуществляется ответственным за обеспечение безопасности ООО КЭМ «Антуриум».

8.7.4. Обработка конфиденциальной информации

При обработке конфиденциальной информации сотрудники обязаны:

- знать и выполнять требования Инструкции по работе с конфиденциальной информацией;
- при необходимости размещать конфиденциальную информацию на открытом ресурсе корпоративной сети ООО КЭМ «Антуриум» применять средства защиты от неавторизованного доступа;
- размещать экран монитора таким образом, чтобы исключить просмотр обрабатываемой информации посторонними лицами;
- не отправлять на печать конфиденциальные документы, если отсутствует возможность контроля вывода на печать и изъятия отпечатанных документов из принтера сразу по окончании печати;
- обязательно проверять адреса получателей электронной почты на предмет правильности их выбора;
- не запускать исполняемые файлы на съемных накопителях, полученные не из доверенного источника;
- не передавать конфиденциальную информацию по открытым каналам связи, кроме сетей корпоративной ИС;

не оставлять без личного присмотра на рабочем месте или где бы то ни было электронные носители информации (CD/DVD – диски, Flash – устройства и пр.), а также распечатки из принтера или бумажные копии документов, содержащие конфиденциальную информацию.

8.7.5. Работа в сети

Доступ к сети Интернет предоставляется сотрудникам ООО КЭМ «Антуриум» в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

Для доступа сотрудников ООО КЭМ «Антуриум» к сети Интернет допускается применение ПО, входящего в Реестр разрешенного к использованию ПО.

При использовании сети Интернет необходимо:

- соблюдать требования настоящей Политики;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность ответственного за обеспечение безопасности о любых фактах нарушения требований настоящей Политики;

При использовании сети Интернет запрещено:

- использовать предоставленный ООО КЭМ «Антуриум» доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;

Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС ООО КЭМ «Антуриум» ;

Публиковать, загружать и распространять материалы содержащие:

Конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с ответственным за обеспечение безопасности;

угрожающую, клеветническую, непристойную информацию;

вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;

фальсифицировать свой IP- адрес, а также прочую служебную информацию.

ООО КЭМ «Антуриум» оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Блокирование и ограничение доступа пользователей к Интернет-ресурсам осуществляется на основе Регламента применения категорий Интернет-ресурсов.

Информация о посещаемых сотрудниками ООО КЭМ «Антуриум» Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству ООО КЭМ «Антуриум» для контроля.

Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

8.7.6. Использование мобильных устройств

Под использованием мобильных устройств и носителей информации в ИС ООО КЭМ «Антуриум»понимается их подключение к инфраструктуре ИС с целью обработки, приема/передачи информации между ИС и мобильными устройствами, а также носителями информации.

На предоставленных ООО КЭМ «Антуриум» мобильных устройствах допускается использование ПО, входящего в Реестр разрешенного к использованию ПО.

К предоставленным ООО КЭМ «Антуриум» мобильным устройствам и носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ. Целесообразность дополнительных мер обеспечения ИБ определяется ответственным за обеспечение безопасности.

При использовании предоставленных ООО КЭМ «Антуриум» мобильных устройств и носителей информации, сотрудник обязан:

соблюдать требования настоящей Политики;

использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;

ставить в известность ответственного за обеспечение безопасности о любых фактах нарушения требований настоящей Политики;

эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;

обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;

извещать ответственного за обеспечение безопасности о фактах утраты (кражи) мобильных устройств и носителей информации.

При использовании предоставленных сотрудника ООО КЭМ «Антуриум» мобильных устройств и носителей информации запрещено:

использовать мобильные устройства и носители информации в личных целях;

передавать мобильные устройства и носители информации другим лицам (за исключением ответственных лиц);

оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, прием\передача информации) инициированное сотрудником ООО КЭМ «Антуриум» между ИС и неучтенными (личными) мобильными устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговоренных с администраторами ИС заранее). ООО КЭМ«Антуриум» оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации;

Информация об использовании сотрудниками ООО КЭМ «Антуриум» мобильных устройств и носителей информации в ИС протоколируется и, при необходимости, может быть представлена ответственному за обеспечение безопасности, а также руководству ООО КЭМ «Антуриум».

Информация, хранящаяся на предоставляемых ООО КЭМ «Антуриум» мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае увольнения, предоставленные ему мобильные устройства и носители информации изымаются.

8.7.7. Защита от вредоносного ПО

Ответственного за обеспечение безопасности регулярно проверяет сетевые ресурсы ООО КЭМ «Антуриум» антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник ООО КЭМ «Антуриум» должен незамедлительно оповестить об этом ответственного за обеспечение безопасности. После чего ответственный за обеспечение безопасности должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

В случае обнаружения при проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники подразделений обязаны:

приостановить работу;

немедленно поставить в известность о факте обнаружения заражения своего руководителя и ответственного за обеспечение безопасности, а также владельца файла и смежные подразделения, использующие эти файлы в работе.

Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

Для предупреждения вирусного заражения рекомендуется:

никогда не открывать файлы и не выполнять макросы, полученные в почтовых сообщениях от неизвестного или подозрительного отправителя. Удалять подозрительные вложения, не открывая их, и очищать корзину, где хранятся удаленные сообщения;

удалять спам, рекламу и другие бесполезные сообщения;

никогда не загружать файлы и программное обеспечение из подозрительных или неизвестных источников;

периодически резервировать важные данные и системную конфигурацию, хранить резервные копии в безопасном месте.

8.8. Приобретение, Разработка и обслуживание систем

8.8.1. Требования безопасности для информационных систем

При описании требований к созданию новых систем или к усовершенствованию существующих необходимо учитывать потребность в средствах обеспечения безопасности.
Требования к безопасности и средств ащиты должны соответствовать ценности используемых ИР и потенциальному ущербу для ООО КЭВ «Антуриум» в случае сбоя или нарушения безопасности. Основой для анализа требований к безопасности и выбору мер для поддержки безопасности является оценка рисков и управление рисками.
Системные требования к ИБ и процессам, обеспечивающим защиту информации, должны быть включены на ранних стадиях проектирования ИС.

8.8.2. Корректная обработка информации

Данные, вводимые в прикладные системы, необходимо проверять, чтобы гарантировать их правильность и соответствие поставленной задаче.

8.8.3. Криптографические средства

Все, поступающие в ООО КЭМ «Антуриум», СКЗИ должны быть учтены в соответствующем журнале поэкземплярного учета СКЗИ.
В ООО КЭМ «Антуриум» должно осуществляться управление ключами для эффективного применения криптографических методов. Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации.
Все ключи должны быть защищены от изменения, утери и уничтожения. Кроме того, секретные и закрытые ключи должны быть защищены от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено.
Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надежности сервиса и времени реакции при предоставлении сервиса.
Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.
Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям, таким как Интернет. Шифрование любой другой информации в ИС ООО КЭМ «Антуриум» должно осуществляться только после получения письменного разрешения на это.

8.8.3.1. Требований по обеспечению ИБ при использовании СКЗИ

Шифрование – это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.
СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Порядок применения СКЗИ определяется руководством ООО КЭМ«Антуриум» и должен включать:

порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;

порядок эксплуатации;

порядок восстановления работоспособности в аварийных случаях;

порядок внесения изменений;

порядок снятия с эксплуатации;

порядок управления ключевой информацией;

порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

Для шифрования конфиденциальной информации минимально допустимой длинной ключа является 128 бит.

При использовании шифрования в ИС ООО КЭМ «Антуриум» должны применяться только утвержденные стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

8.8.3.2. Электронные цифровые подписи

ЭЦП обеспечивают защиту аутентификации и целостности электронных документов.

ЭЦП могут применяться для любой формы документа, обрабатываемого электронным способом. ЭЦП должны быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой – для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

Криптографические ключи, используемые для цифровых подписей, должны отличаться от тех, которые используются для шифрования.

При использовании ЭЦП, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

8.8.3.1. Управление ключами

Управление криптографическими ключами важно для эффективного использования криптографических средств.

Любая компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации. Следует применять систему защиты для обеспечения использования в ИС ООО КЭМ «Антуриум» криптографических методов в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами должны использоваться для шифрования и для генерации цифровых подписей.

Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия. Криптографические методы могут также использоваться для этой цели. Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Сервер сертифицированного центра КУЦ должен хранить текущие открытые ключи для всех авторизованных на это сотрудников. Для безопасного взаимодействия с внешними пользователями ИС ООО КЭМ «Антуриум» необходимо использовать электронные сертификаты только из утвержденного списка сертифицированных центров.

Секретные ключи пользователей должны храниться так же, как и пароли. О любом подозрении на компрометацию секретного ключа пользователь должен немедленно доложить ответственному за обеспечение безопасности.

Необходимо, чтобы система обеспечения безопасности использования ключей основывалась на согласовании способов, процедур и безопасных методов для:

генерации ключей при использовании различных криптографических систем и приложений;

генерации и получения сертификатов открытых ключей;

рассылки ключей, предназначенных пользователям, включая инструкции по их активации при получении;

хранения ключей (при этом необходимо наличие инструкции авторизованным пользователям для получения доступа к ключам);

смены или обновления ключей, включая правила порядка и сроков смены ключей;

порядка действий в отношении скомпрометированных ключей;

аннулирования ключей, в том числе способы аннулирования или дезактивации ключей, если ключи были скомпрометированы или пользователь уволился из организации (в этом случае ключи необходимо архивировать);

восстановление ключей, которые были утеряны или испорчены, для рассекречивания зашифрованной информации;

архивирования и резервного копирования ключей;

разрушения ключей;

регистрация ключей и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации, для ключей необходимо определить даты начала и конца действия, чтобы их можно было использовать лишь в течении ограниченного периода времени, который зависит от обстоятельств использования криптографических средств, контроля и от степени риска раскрытия информации.

Может потребоваться наличие процедур обработки юридических запросов, касающихся доступа к криптографическим ключам, например, чтобы зашифрованная информация стала доступной в незашифрованном виде для доказательств в суде.

Необходимо обеспечивать защиту открытых ключей от угроз подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей. Сертификаты необходимо изготавливать таким способом, который однозначно связывал бы информацию, относящуюся к владельцу пары открытого/секретного ключей, с открытым ключом. Поэтом важно, чтобы процессу управления, в рамках которого формируются эти сертификаты, можно было доверять.

Соглашения с внешними поставщиками криптографических услуг (например, с удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надежности сервиса и времени реакции при предоставлении сервиса.

8.8.4. Безопасность системных файлов

Чтобы свести к минимуму риск повреждения ИС, в ООО КЭМ «Антуриум» необходимо обеспечить контроль над внедрением ПО в рабочих системах.

Тестовые данные должны находиться под контролем и защитой. Для испытаний обычно требуются значительные объемы тестовых данных, максимально близко соответствующие рабочим данным. Необходимо избегать использования рабочих баз данных, содержащих конфиденциальную информацию. Если эти базы все же будут использоваться, то конфиденциальные данные должны быть удалены или изменены.

8.8.5. Безопасность процесса разработки и обслуживания систем

Чтобы свести к минимуму вероятность повреждения ИС ООО КЭМ «Антуриум», следует ввести строгий контроль над внесением изменений. Необходимо установить официальные правила внесения изменений. Эти правила должны гарантировать, что процедуры, связанные с безопасностью и контролем, не будут нарушены, что программисты, занимающиеся поддержкой, получат доступ только к тем частям системы, которые необходимы для их работы, и что для выполнения любого изменения требуется получить официальное разрешение и подтверждение.

После внесения изменений в ИС критичные для бизнес-процессов ООО КЭМ «Антуриум»приложения должны анализироваться и тестироваться, чтобы гарантировать отсутствие вредных последствий для безопасности ООО КЭМ «Антуриум».

Следует препятствовать внесению изменений в пакеты ПО, за исключением необходимых изменений. Все изменения должны строго контролироваться.

8.9. Управление инцидентами информационной безопасности

В ООО КЭМ «Антуриум» должна быть разработана и утверждена формальная процедура уведомления о происшествиях в области ИБ, а также процедура реагирования на такие происшествия, включающая в себя действия, которые должны выполняться при поступлении сообщений о происшествии.

Все сотрудники должны быть ознакомлены с процедурой уведомления, а в их обязанности должна входить максимально быстрая передача информации о происшествиях.

В дополнение к уведомлению о происшествиях ИБ и недостатках безопасности должен использоваться мониторинг систем, сообщений и уязвимостей для обнаружения инцидентов ИБ.

Цели управления инцидентами ИБ должны быть согласованы с руководством для учета приоритетов ООО КЭМ «Антуриум» при обращении с инцидентами.

Необходимо создать механизмы, позволяющие оценивать и отслеживать типы инцидентов, их масштаб и связанные с ними затраты.

8.10. Управление непрерывностью и восстановлением

Необходимо разработать контролируемый процесс для обеспечения и поддержки непрерывности бизнес-процессов ООО КЭМ «Антуриум». Данный процесс должен объединять в себе основные элементы поддержки непрерывности бизнес-процессов.

В ООО КЭМ «Антуриум» должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес-процессов.

В каждом плане поддержки непрерывности бизнеса должны быть четко указаны условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.

Для каждого плана должен быть назначен определенный владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

8.11. Соблюдение требований законодательства

Все значимые требования, установленные действующим законодательством, подзаконными актами и договорными отношениями, а также подход ООО КЭМ «Антуриум» к обеспечению соответствия этим требованиям должны быть явным образом определены, документированы и поддерживаться в актуальном состоянии.

Необходимо соблюдение регламентированного процесса, предупреждающего нарушение целостности, достоверности и конфиденциальности ИР, содержащих персональные данные, начиная от стадии сбора и ввода данных до их хранения. Персональные данные конкретного сотрудника и процесс их обработки должен быть открытым для этого сотрудника.

В Учреждении должны быть внедрены соответствующие процедуры для обеспечения соблюдения законодательных ограничений, подзаконных актов и контрактных обязательств по использованию материалов, охраняемых авторским правом, а также по использованию лицензионного ПО.

Важная документация ООО КЭМ «Антуриум» должна быть защищена от утери, уничтожения и фальсификации в соответствии с требованиями законодательства, подзаконных актов, контрактных обязательств и бизнес-требований.

Система хранения и обработки должна обеспечивать четкую идентификацию записей и их периода хранения в соответствии с требованиями законов и нормативных актов. Эта система должна иметь возможность уничтожения записей по истечении периода хранения, если эти записи больше не требуются ООО КЭМ «Антуриум».

Криптографические средства должны использоваться в соответствии со всеми имеющимися соглашениями, законодательными и нормативными актами.

8.12. Аудит информационной безопасности

ООО КЭМ «Антуриум» должно проводить внутренние проверки СУИБ через запланированные интервалы времени.

Основные цели проведения таких проверок:

- оценка текущего уровня защищенности ИС;
- выявление и локализация уязвимостей в системе защиты ИС;
- анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ИС;
- оценка соответствия ИС требованиям настоящей Политики;
- выработка рекомендаций по совершенствованию СУИБ за счет внедрения новых и повышения эффективности существующих мер защиты информации.

В число задач, решаемых при проведении проверок и аудитов СУИБ, входят:

- сбор и анализ исходных данных об организационной и функциональной структуре ИС, необходимых для оценки состояния ИБ;
- анализ существующей политики безопасности и других организационно-распорядительных документов по защите информации на предмет их полноты и эффективности, а также формирование рекомендаций по их разработке (или доработке);
- технико-экономическое обоснование механизмов безопасности;
- проверка правильности подбора и настройки средств защиты информации, формирование предложений по использованию существующих и установке дополнительных средств защиты для повышения уровня надежности и безопасности ИС;
- разбор инцидентов ИБ и минимизация возможного ущерба от их проявления.

Руководство и сотрудники ООО КЭМ «Антуриум» при проведении у них аудита СУИБ обязаны оказывать содействие аудиторам и предоставлять всю необходимую для проведения аудита информацию.

8.13. Предоставление услуг сторонним организациям

8.13.1. Соглашения о предоставлении услуг

В соглашения о предоставлении услуг сторонним организациям должны быть включены требования безопасности, описание, объемы и характеристики качества предоставляемых услуг.

8.13.2. Анализ предоставления услуг

Услуги, отчеты и записи, предоставляемые сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

контроль объема и качества услуг, оговоренных в соглашениях;
предоставление сторонней организации информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
анализ предоставленных сторонними организациями отчетов о предоставленных услугах;
управление любыми обнаруженными проблемами.

8.13.3. Приемка систем

В ООО КЭМ«Антуриум» должен быть разработан и утвержден порядок приемки новых ИС, обновления и новых версий ПО.

9. Ответственность

Главный врач ООО КЭМ «Антуриум» определяет приоритетные направления деятельности в области обеспечения ИБ, меры по реализации настоящей Политики, утверждает списки объектов и сведений, подлежащих защите, а также осуществляет общее руководство обеспечением ИБ ООО КЭМ «Антуриум».
Ответственность за поддержание положений настоящей Политики в актуальном состоянии, создание, внедрение, координацию и внесение изменений в процессы СУИБ ООО КЭМ «Антуриум» лежит на ответственном за организацию обработки ПДн и ответственном за обеспечение безопасности ПДн.
Все руководители несут прямую ответственность за реализацию Политики и ее соблюдение персоналом в соответствующих подразделениях.
Работники ООО КЭМ «Антуриум» несут персональную ответственность за соблюдение требований документов СУИБ и обязаны сообщать обо всех выявленных нарушениях в области информационной безопасности ответственному за обеспечение безопасности.
В трудовых договорах и должностных инструкциях работников устанавливается ответственность за сохранность служебной информации, ставшей известной в силу выполнения своих обязанностей.
Руководство ООО КЭМ «Антуриум» регулярно проводит совещания, посвященные проблемам обеспечения информационной безопасности с целью формирования четких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.
Нарушение требований нормативных актов ООО КЭМ «Антуриум» по обеспечению ИБ является чрезвычайным происшествием и будет служить поводом и основанием для проведения служебного расследования.

10. Контроль и пересмотр

Общий контроль состояния ИБ ООО КЭМ «Антуриум» осуществляется ответственным за организацию обработки ПДн.

Текущий контроль соблюдения настоящей Политики осуществляет ответственный за обеспечение безопасности ПДн. Контроль осуществляется путем проведения мониторинга и менеджмента инцидентов ИБ ООО КЭМ «Антуриум», по результатам оценки ИБ, а также в рамках иных контрольных мероприятий.

Ответственные лица ежегодно пересматривает положения настоящей политики и вносят соответствующие изменения.

Порядок пересмотра документов второго и третьего уровней определяется в данных документах.

Все изменения, внесенные в настоящую Политику ИБ должны учитываться в листе «История изменений».

11. История изменений

Версия	Дата утверждения	Изменения	Кто внес изменения
1.0		Первоначальная редакция	