



КОНЦЕПЦИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГАУ «Республиканский медицинский библиотечно-информационный центр»

1 ОБЩИЕ ПОЛОЖЕНИЯ

- 1.1 Информация о документе, разработчиках, порядке согласования, порядке пересмотра и утверждения.

2 НАЗНАЧЕНИЕ

- 2.1 Настоящий документ определяет концепцию информационной безопасности в рамках Системы управления информационной безопасностью ГАУ «РМБИЦ» как систему документированных управленческих решений, направленных на защиту определенных защищаемых ресурсов РМБИЦ.
- 2.2 Настоящий документ устанавливает порядок и состав мероприятий по обеспечению информационной безопасности и предназначен для выполнения персоналом, участвующем в процессах обеспечения информационной безопасности.
- 2.3 Настоящий документ разработан с целью установления единого подхода персоналом РМБИЦ, участвующим в процессах управления информационной безопасностью, в соответствии с требованиями международного стандарта.

3 ОБЛАСТЬ ПРИМЕНЕНИЯ

- 3.1 Настоящий документ обязателен для применения во всех подразделениях и всеми должностными лицами ГАУ «РМБИЦ» при управлении информационной безопасностью.
- 3.2 Действие настоящего документа распространяется на деятельность всех подразделений РМБИЦ.

4 НОРМАТИВНЫЕ ССЫЛКИ

- 4.1 При разработке настоящей Концепции использованы следующие нормативные документы:

5 ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

- 5.1 *Информационная система* - совокупность компонентов, состоящая из одного или более процессов, аппаратных средств, программного обеспечения, оборудования и людей, услуг, обеспечивающая возможность удовлетворения установленных потребностей или целей.
- 5.2 *Программный продукт* - программное обеспечение или связанная с ним информация, созданное, модифицированное или встроенное в соответствии с условиями контракта (договора) потребителя;
- 5.3 *Программное обеспечение* - компьютерные программы и базы данных;
- 5.4 *Изделие программного обеспечения* - любая, поддающаяся идентификации, часть программного обеспечения на промежуточном или конечном этапе разработки;
- 5.5 *Программный документ* - документ, содержащий сведения, необходимые для обеспечения функционирования и эксплуатации программного продукта;

- 5.6 *Инструкция* - нормативный документ, в котором подробно описано детальное выполнение отдельных действий;
- 5.7 *Методика* - нормативный документ, в котором подробно изложен установленный способ осуществления деятельности;
- 5.8 *Нормативный документ* - документ, устанавливающий правила, общие принципы или характеристики, касающиеся различных видов деятельности или их результатов;
- 5.9 *Доступность* – элемент информационной безопасности;
- 5.10 *Конфиденциальность* – элемент информационной безопасности;
- 5.11 *Данные* - представление фактов, понятий и инструкций в нормализованном виде, подходящем для передачи, интерпретации и обработки человеком или машиной;
- 5.12 *Информация* - смысл, который в настоящее время придаётся данным, посредством соответствующих соглашений;
- 5.13 *Информационная безопасность* - защита информации, её составляющие:
 - 5.13.1 *конфиденциальность* - защита конфиденциальной информации от несанкционированного раскрытия или перехвата;
 - 5.13.2 *целостность*: обеспечение точности и полноты информации и компьютерных программ;
 - 5.13.3 *доступность*: обеспечение доступности информации и жизненно важных сервисов для пользователя, когда это требуется.
- 5.14 *Управление информационной безопасностью* - Обеспечение механизма, позволяющего реализовать информационную безопасность.
- 5.15 *Информационная технология* - Научная, технологическая и инженерная дисциплина и управление методами, используемыми для оперирования с данными и их обработки; их прикладное применение; компьютеры и их взаимодействие с человеком и машинами; а также связанные с этим социальные, экономические и культурные вопросы.
- 5.16 *Целостность* - Элемент информационной безопасности.
- 5.17 *Владелец* - Лицо или организация, отвечающая за определённые информационные ресурсы и за реализацию надлежащих защитных мер.
- 5.18 *Анализ рисков* - Всеобъемлющий термин, включающий, во-первых, определение и анализ потенциальных угроз, которым подвергаются компьютерные системы, и их уязвимости, и, во-вторых, предоставление руководству информации, необходимой для принятия решений, связанных с оптимизацией капиталовложений в меры по обеспечению информационной безопасности.
- 5.19 *Инцидент в системе безопасности* - Событие, в результате которого произошла (или могла бы произойти) потеря или повреждение информационных ресурсов организации, либо действие, которое нарушает принятые в организации правила безопасности.
- 5.20 *Специальная привилегия* - Любая особенность или средство многопользовательской информационной системы, дающая возможность пользователю обойти средства контроля системы или приложения.
- 5.21 *Пользователь* - Лицо или организация, использующая информационные технологии.

6 УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

- 6.1 Концепция информационной безопасности – стратегические правила, которые должны соблюдаться в повседневной деятельности РМБИЦ. Концепция информационной безопасностью определяет общие принципы и стандарты работы и служит основанием для разработки и выполнения процедур информационной безопасности.
- 6.2 Основными целями процесса управления информационной безопасностью является поддержание конфиденциальности, целостности и доступности информационных

- активов РМБИЦ, минимизация влияния инцидентов, связанных с повреждением или уничтожением информационных активов РМБИЦ.
- 6.3 Ответственным за процесс является заведующий WEB –узла и главный инженер.
 - 6.4 Объектами защиты являются информационные активы, определенные в рамках процесса управления информационной безопасностью.
 - 6.5 Задачами процесса управления информационной безопасностью являются:
 - 6.5.1 Осуществление конкретных мероприятий по защите информационных активов от несанкционированного использования, открытия или случайного уничтожения;
 - 6.5.2 Обеспечение целевого и согласованного с руководством использования информационных активов РМБИЦ;
 - 6.5.3 Осуществление конкретных мероприятий по защите информационных активов от несанкционированного использования, открытия или случайного уничтожения
 - 6.5.4 Мониторинг отклонений от установленных защитных практик и проведение корректирующих и предупреждающих действий по результатам анализа мониторинга;
 - 6.5.5 Осуществление конкретных мероприятий по защите информационных активов от несанкционированного использования, открытия или случайного уничтожения;
 - 6.5.6 Актуализация Концепции информационной безопасности в соответствии с отчетами и анализом руководства.
 - 6.6 Определены следующие типы информации:
 - 6.6.1 Информация общего пользования (без указания ограничений);
 - 6.6.2 Информация ограниченного пользования (ограничение указывается в обязательном порядке), которая может быть:
 - 6.6.2.1 Информацией на рабочем месте сотрудника;
 - 6.6.2.2 Информацией для внутреннего пользования;
 - 6.6.2.3 Информацией, касающаяся второй стороны (заказчики и партнеры).
 - 6.7 В рамках Концепции информационной безопасности сотрудники ГАУ «РМБИЦ» обязаны соблюдать следующие положения.
 - 6.7.1 Сотрудники обязаны менять пароли доступа на свое рабочее место не реже 1 раза в год во избежание потери информации, а также предоставления доступа к ресурсам РМБИЦ неавторизованным или сторонним пользователям;
 - 6.7.2 Сотрудники обязаны контролировать документы на своих рабочих местах и в случае отсутствия на рабочем месте убирать документы ограниченного пользования в места, недоступные неавторизованным или сторонним пользователям (политика «чистого стола»);
 - 6.7.3 Сотрудники обязаны на время отсутствия на своем рабочем месте вне зависимости от длительности периода отсутствия блокировать доступ к ресурсам своего рабочего места (политика «чистого экрана»);
 - 6.7.4 Сотрудники ГАУ «РМБИЦ» при устройстве на работу подписывают трудовой договор и в рамках трудового договора обязаны соблюдать практику целевого использования ресурсов (ресурсы Интернет, электронная почта);
 - 6.7.5 Сотрудники РМБИЦ при устройстве на работу в обязательном порядке подписывают Соглашение о конфиденциальности, которое позволяет им работать с информацией общего и ограниченного пользования.
 - 6.8 Во избежание неавторизованного доступа в помещения ГАУ «РМБИЦ», к инфраструктуре, введено ограничения физического доступа в РМБИЦ. В связи с этим
 - 6.8.1 Составлен перечень помещений с ограниченным доступом (Приложение № 4).

- 6.8.2 Составлен список сотрудников имеющих доступ в помещения с ограниченным доступом (Приложение № 2).
- 6.8.3 Перемещение лиц, не являющихся сотрудниками РМБИЦ возможно только в сопровождении сотрудника учреждения.
- 6.9 В рамках Концепции информационной безопасности проводятся следующие мероприятия:
 - 6.9.1 идентификация наиболее ценных активов РМБИЦ;
 - 6.9.2 оценка рисков, связанных с потерями или повреждением наиболее ценных активов РМБИЦ;
 - 6.9.3 принятие управленческих решений о защите активов на основании проведенной оценки рисков;
 - 6.9.4 регистрация и контроль инцидентов информационной безопасности;
 - 6.9.5 предоставление отчетности по инцидентам, связанным с информационной безопасностью;
 - 6.9.6 предоставление отчетности о деятельности процесса управления информационной безопасностью;
 - 6.9.7 проведение руководством анализа отчетов с целью получения информации о процессе управления информационной безопасностью и принятия решения о пересмотре основных активов и рисков;
 - 6.9.8 пересмотр на регулярной основе активов и рисков;
 - 6.9.9 усовершенствование (развитие) процесса.
- 6.10 Целевые показатели процесса Управления информационной безопасностью:
 - 6.10.1 количество инцидентов информационной безопасности за год не должно превышать 1 инцидента для каждого актива, подлежащего контролю;
- 6.11 Роли участников процесса
 - 6.11.1 Процесс управления информационной безопасностью предполагает следующее разделение участников по ролям:
 - 6.11.1.1 Заместитель директора по ИБР;
 - 6.11.1.2 Главный инженер.
- 6.12 Порядок вступления в силу и пересмотра Концепции информационной безопасности.
 - 6.12.1 Концепция информационной безопасности вступает в силу со дня утверждения документа директором.
 - 6.12.2 Концепция информационной безопасности пересматривается не реже 1 раза в год или по требованию руководства.

7

ЗАЩИТА ИНФОРМАЦИИ НА ДИСКОВЫХ НОСИТЕЛЯХ

- 7.1 Защита информации на серверах.
 - 7.1.1 Запрещено предоставлять доступ к конфиденциальной информации (КИ) лицам, чья деятельность не подразумевает ознакомления с таковой. Список лиц составляется руководителями подразделений и утверждается у вышестоящего руководства РМБИЦ.
 - 7.1.2 Для исключения потери информации из-за поломки оборудования или в виду воздействия третьих сил, необходимо регулярно резервировать информацию, хранимую на серверах.
 - 7.1.3 Запрещено хранение КИ на общих ресурсах, вместе с не конфиденциальной информацией (НКИ).
 - 7.1.4 Использовать для хранения КИ PGP крипто диски (или крипто диски другой разработки).
- 7.2 Защита информации на рабочих местах пользователей.
 - 7.2.1 Запрещено хранить (КИ) на съёмных носителях на рабочих местах пользователей и на персональных компьютерах пользователей, а также на мобильных персональных компьютерах.

