Краевое государственное бюджетное учреждение здравоохранения
«Красноярская станция скорой медицинской помощи»
(КГБУЗ «КССМП»)

ПРИКАЗ

05.08.2025 № 209 -пр.

Об утверждении политики
Информационной безопасности

В целях соблюдения требований информационной безопасности учреждения

ПРИКАЗЫВАЮ:

Утвердить:

1. Политика информационной безопасности КГБУЗ «КССМП».
2. Довести данную политику до ответственных лиц, внедрить в работу в срок до 20.08.2025 года.
3. Контроль за исполнением приказа возложить на исполняющего обязанности главного врача по ОМР Мандрык Е.В.

Главный врач С.А. Скрипкин

УТВЕРЖДЕН

Приказом № 209-пр

от 05.08.2025 г.

ПОЛИТИКА

информационной безопасности КГБУЗ «КССМП»

Дата введения в действие:

20.08.2025 г.

Красноярск, 2025г.

ЛИСТ СОГЛАСОВАНИЯ:

Ответственность	Должность	Фамилия, инициалы	Подпись	Дата
Согласовал	Исполняющий обязанности заместителя главного врача по ОМР	Мандрык Е.В.		04.08.2025
Согласовал	Начальник отдела правовой и кадровой работы	Репис Е.В.		04.08.2025
Разработал	Начальник отдела АСУ	Кулешов А.Б.		04.08.2025

***документ создан совместно с Центром компетенций КГБУЗ «ККБ»**

1 СОКРАЩЕНИЯ И ОБОЗНАЧЕНИЯ

АС – автоматизированная система;
АСУ – автоматизированная система управления;
ИБ – информационная безопасность;
ИС – информационная система;
ИТ – информационная технология;
КГБУЗ КССМП (Учреждение) – Краевое государственное бюджетное учреждение здравоохранения «Красноярская станция скорой медицинской помощи»;
ОЗ – объект защиты;
СЗИ – средства защиты информации;
СОИБ – система обеспечения информационной безопасности;
ТП – технологический процесс.

2 ОБЩИЕ ПОЛОЖЕНИЯ

Настоящая политика является основополагающим документом, предназначенным для определения целей, задач, принципов и подходов в области информационной безопасности.

Требования настоящей Политики обязательны для исполнения всеми работниками КГБУЗ КССМП, а также иными лицами, получившими доступ к объектам защиты КГБУЗ КССМП. Указанные лица должны быть ознакомлены с настоящей Политикой до получения доступа к объектам защиты.

3 НОРМАТИВНЫЕ ССЫЛКИ

Настоящая Политика разработана на основании следующих нормативных правовых актов:

–ГОСТ Р ИСО/МЭК 27001-2021. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования;

– ГОСТ Р ИСО/МЭК 27002-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности;

– ГОСТ Р ИСО/МЭК 27003-2021. Национальный стандарт Российской Федерации. Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации;

– Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ;

– Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ;

– Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 N 187-ФЗ;

– Указ Президента Российской Федерации от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»;

– Приказ ФСТЭК России от 18.02.2013 N 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

– Приказ ФСТЭК России от 21.12.2017 N 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»;

– Приказ ФСТЭК России от 25.12.2017 N 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

4 ЦЕЛИ, ЗАДАЧИ И ПРИНЦИПЫ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Целью КГБУЗ КССМП в области информационной безопасности является снижение информационных рисков до уровня, позволяющего осуществлять устойчивое функционирование КГБУЗ КССМП, а также создания условий достижения стратегических целей КГБУЗ КССМП.

Задачи в области информационной безопасности:

– определение контекста деятельности организации;

– определение источников требований в области информационной безопасности для КГБУЗ КССМП;

– определение и классификация объектов защиты, их условий эксплуатации (функционирования);

– оценка информационных рисков;

– определение требований по обеспечению информационной безопасности для КГБУЗ КССМП;

– аудит соответствия требованиям по обеспечению информационной безопасности для существующих систем обеспечения информационной безопасности;

– разработка системы обеспечения информационной безопасности для объектов защиты;

– реализация системы обеспечения информационной безопасности для объектов защиты;

– сопровождение системы обеспечения информационной безопасности объектов защиты в ходе её эксплуатации;

– обнаружение и расследование инцидентов информационной безопасности;

– взаимодействие с внешними сторонами, заинтересованными в обеспечении информационной безопасности КГБУЗ КССМП;

– контроль эффективности функционирования системы обеспечения информационной безопасности объектов защиты;

– принятие мер по повышению эффективности системы обеспечения информационной безопасности.

Принципы обеспечения информационной безопасности.

Принцип законности.

При планировании и реализации мероприятий по обеспечению информационной безопасности, должны быть выполнены требования действующего законодательства Российской Федерации.

Планирование и реализация мероприятий по обеспечению информационной безопасности осуществляется с документированием перечня мер, способов реализации и результатов реализации данных мер, в порядке установленном действующим законодательством Российской Федерации и локальными нормативными актами Учреждения.

Принятые меры по защите информации должны учитывать предоставление доступа к объектам защиты должностным лицам федеральных органов исполнительной власти, в соответствии с Порядком предоставления доступа должностным лицам федеральных органов исполнительной власти к объектам критической информационной инфраструктуры КГБУЗ КССМП и действующим законодательством Российской федерации.

Средства, используемые для реализации мероприятий по обеспечению информационной безопасности, должны соответствовать требованиям, установленным действующим законодательством Российской Федерации к средствам защиты информации.

Принцип непрерывности.

Процессы планирования и реализации мероприятий по обеспечению информационной безопасности, должны осуществляться непрерывно, в рамках установленного цикла, на всех этапах жизненного цикла объекта защиты.

Разработанные планы мероприятий должны непрерывно приходить на смену друг другу.

Принцип системности.

При реализации мероприятий по обеспечению информационной безопасности необходимо применять системный подход, который предполагает сохранение взаимосвязей процессов, участниками которых являются объекты защиты, а также применение методов и средств защиты информации, совместимых между собой.

Принцип превентивности.

Мероприятия по обеспечению информационной безопасности, преимущественно, должны быть направлены на предотвращение реализации соответствующих угроз информационной безопасности объектов защиты.

Принцип многоуровневости.

При реализации мероприятий по обеспечению информационной безопасности необходимо, применять единые средства обеспечения информационной безопасности с целью организации централизованного управления компонентами обеспечения информационной безопасности.

Допустимо применение разнородных средств обеспечения информационной безопасности с целью построения целостной системы обеспечения информационной безопасности и устранения уязвимостей.

При реализации мероприятий по обеспечению информационной безопасности необходимо применение эшелонированных средств обеспечения информационной безопасности нескольких уровней, имеющих различную логику построения защитных механизмов.

Принцип целесообразности.

Количество ресурсов, затраченных на обеспечение информационной безопасности, не должно превышать размер ущерба, теоретически полученного от недостаточной реализации этих мер.

Принцип профессионализма.

Штатные работники структурного подразделения, на которое возложены функции по обеспечению информационной безопасности, должны иметь профессиональное образование по направлению подготовки в области информационной безопасности или иное высшее профессиональное образование с прохождением обучения по программе повышения квалификации по направлению «Информационная безопасность».

В случае необходимости допустимо привлечение организаций к осуществлению мероприятий по обеспечению информационной безопасности КГБУЗ КССМП. При этом могут привлекаться исключительно организации, имеющие лицензии на осуществление соответствующего вида деятельности.

В случае необходимости допустимо привлечение организаций к осуществлению мероприятий по обнаружению, предупреждению и ликвидации последствий компьютерных атак, и реагированию на компьютерные инциденты. При этом могут привлекаться исключительно организации, являющиеся аккредитованными центрами государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.

Принцип наименьших полномочий.

Пользователи и сущности в информационной системе должны быть обеспечены правами доступа, минимально достаточными для выполнения ими своих должностных обязанностей.

Повышение прав доступа осуществляется только при наличии обоснования на использование информации, ознакомление с информацией, подключение к информационной системе, а также при наличии согласования на выполнение действий от непосредственного руководителя работника, запрашивающего доступ.

Принцип разделения и актуализации полномочий.

При реализации мероприятий по обеспечению информационной безопасности необходимо разделять полномочия работников, с целью минимизации вероятности совершения ошибок работником, которому предоставлен широкий перечень полномочий.

При изменении должности и (или) функциональных обязанностей работника, необходимо выполнять пересмотр прав доступа данного работника к информационным ресурсам, с целью исключения избыточности прав доступа к информационным ресурсам.

5 ПОДХОДЫ К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1. Объектом защиты является информация, носитель информации, информационный процесс, или субъект, которые необходимо защищать в соответствии с целью защиты информации, установленной действующим законодательством Российской Федерации в области информационной безопасности. Объекты защиты определяются руководителем КГБУЗ КССМП.

5.2. Системы обеспечения информационной безопасности создаются в отношении объектов защиты Учреждения и включают в себя правовые, организационные, технические и иные меры, направленные на достижение целей информационной безопасности.

5.3. СОИБ включают силы обеспечения информационной безопасности и используемые ими средства обеспечения информационной безопасности. К силам обеспечения информационной безопасности относятся:

– подразделения (работники), ответственные за обеспечение информационной безопасности;

– подразделения (работники), эксплуатирующие объекты защиты;

– подразделения (работники), обеспечивающие функционирование (сопровождение, обслуживание, ремонт) объектов защиты;

– иные подразделения (работники), участвующие в обеспечении информационной безопасности объектов защиты.

5.4 К средствам обеспечения информационной безопасности относятся программные и программно-аппаратные средства, применяемые для обеспечения информационной безопасности.

5.5. СОИБ должны функционировать в соответствии с организационно-распорядительными документами по обеспечению информационной безопасности, разрабатываемыми в соответствии с требованиями законодательства РФ.

5.6. Создаваемые СОИБ должны соответствовать требованиям, предъявляемым к:

– силам обеспечения информационной безопасности;

– программным и программно-аппаратным средствам, применяемым для обеспечения информационной безопасности;

– организационно-распорядительным документам по информационной безопасности;

– функционированию СОИБ.

5.7. Требования к силам обеспечения информационной безопасности.

5.7.1. Силами обеспечения информационной безопасности являются работники Учреждения, государственные органы, уполномоченные на решение задач по обеспечению информационной безопасности, в соответствии с действующим законодательством Российской Федерации и сторонние организации, имеющие договорные отношения с Учреждением, в части обеспечения информационной безопасности.

5.7.2. С целью создания системы безопасности объектов защиты, организации и контролю ее функционирования, полномочия по обеспечению информационной безопасности возлагаются приказом на заместителя руководителя Учреждения.

5.7.3. Руководитель Учреждения создает или определяет структурное подразделение, ответственное за обеспечение информационной безопасности объектов защиты Учреждения.

5.7.4. Структурное подразделение, ответственное за обеспечение информационной безопасности реализует функции по обеспечению безопасности объектов защиты при взаимодействии с подразделениями (работниками), эксплуатирующими объекты защиты, и подразделениями (работниками), обеспечивающими функционирование объектов защиты.

5.7.5. В целях реализации информационной безопасности, Учреждения могут привлекаться организации, имеющие, лицензию на деятельность по технической защите конфиденциальной информации

5.8. Требования к средствам обеспечения информационной безопасности.

5.8.1. Средствами обеспечения информационной безопасности являются программные и программно-аппаратные решения, к которым относятся средства защиты информации, в том числе средства защиты информации от несанкционированного доступа (включая встроенные в общесистемное, прикладное программное обеспечение), межсетевые экраны, средства обнаружения (предотвращения) вторжений (компьютерных атак), средства антивирусной защиты, средства защиты каналов передачи данных.

5.8.2. Параметры и характеристики применяемых средств защиты информации должны обеспечивать реализацию технических мер по обеспечению безопасности объектов защиты, принимаемыми в соответствии с требованиями по безопасности, предъявляемыми к Учреждению.

5.8.3. Средства защиты информации должны применяться в соответствии с инструкциями (правилами) по эксплуатации, разработанными разработчиками (производителями) этих средств, и иной эксплуатационной документацией на средства защиты информации.

5.8.4. Применяемые средства защиты информации должны быть обеспечены технической поддержкой со стороны разработчиков (производителей).

5.8.5. При выборе средств защиты информации должно учитываться возможное наличие ограничений со стороны разработчиков (производителей) или иных лиц на применение этих средств на любом из объектов защиты Учреждения.

5.8.6. В случае невозможности обеспечения средств защиты информации технической поддержкой со стороны разработчиков (производителей), Учреждением должны быть реализованы организационные и технические меры, обеспечивающие блокирование (нейтрализацию) угроз безопасности информации объекта защиты, в соответствии с предъявляемыми Требованиями по обеспечению безопасности данного объекта защиты.

5.8.7. Порядок применения средств защиты информации определяется Учреждением в соответствии с ежегодным планом мероприятий по обеспечению безопасности объектов защиты Учреждения.

5.9. Требования к организационно-распорядительным документам по информационной безопасности.

5.9.1. В рамках функционирования системы безопасности, Учреждением должны быть утверждены организационно-распорядительные документы по безопасности объектов защиты, которые эксплуатируются в подразделениях Учреждения, определяющие

порядок и правила функционирования системы безопасности объектов защиты, а также порядок и правила обеспечения безопасности объектов защиты.

5.9.2. Организационно-распорядительные документы по безопасности объектов защиты являются частью документов по вопросам обеспечения информационной безопасности (защиты информации) Учреждения.

5.9.3. Организационно-распорядительные документы по безопасности значимых объектов разрабатываются с учетом особенностей деятельности субъекта критической информационной инфраструктуры на основе требований по безопасности.

5.9.4. Организационно-распорядительные документы по безопасности объектов защиты должны определять:

– цели и задачи обеспечения безопасности объектов защиты, основные угрозы безопасности информации и категории нарушителей, основные организационные и технические мероприятия по обеспечению безопасности объектов защиты, проводимые Учреждением, состав и структуру системы безопасности и функции ее участников, порядок применения, формы оценки соответствия объектов защиты и средств защиты информации требованиям по безопасности;

– планы мероприятий по обеспечению безопасности объектов защиты, модели угроз безопасности информации, порядок реализации отдельных мер по обеспечению безопасности объектов защиты, порядок проведения испытаний или приемки средств защиты информации, порядок реагирования на компьютерные инциденты, порядок информирования и обучения работников, порядок взаимодействия подразделений (работников) Учреждения при решении задач обеспечения безопасности объектов защиты, порядок взаимодействия Учреждения с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации;

– правила безопасной работы работников Учреждения на объектах защиты, действия работников Учреждения при возникновении компьютерных инцидентов и иных нештатных ситуаций.

5.9.5. Организационно-распорядительные документы по безопасности объектов защиты утверждаются главным врачом Учреждения. По решению главного врача Учреждения отдельные организационно-распорядительные документы по безопасности объектов защиты могут утверждаться иными уполномоченными работниками Учреждения.

5.9.6. Организационно-распорядительные документы по безопасности объектов защиты должны быть доведены до руководства Учреждения, ответственного лица, подразделения по безопасности, специалистов по безопасности, а также до иных подразделений (работников), участвующих в обеспечении безопасности объектов защиты, в части, их касающейся.

5.10. В рамках реализации функционирования СОИБ. должно быть предусмотрено:

– планирование, разработка, совершенствование и осуществление внедрения мероприятий по обеспечению информационной безопасности объектов защиты Учреждения;

– принятие организационных и технических мер для обеспечения информационной безопасности объектов защиты Учреждения;

– установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения информационной безопасности объектов защиты Учреждения.

Планирование и разработка мероприятий по обеспечению информационной безопасности объектов защиты Учреждения.

5.10.1. В рамках планирования мероприятий по обеспечению информационной безопасности объектов защиты Учреждения осуществляются разработка и утверждение ежегодного плана мероприятий по обеспечению безопасности объектов защиты Учреждения (далее – план мероприятий). При необходимости, план мероприятий может разрабатываться на более длительный срок.

План мероприятий должен содержать наименования мероприятий по обеспечению безопасности объектов защиты Учреждения, сроки их выполнения, наименования подразделений (работников), ответственных за реализацию каждого мероприятия.

Разработка мероприятий по обеспечению безопасности объектов защиты осуществляется в соответствии с Требованиями действующего законодательства Российской Федерации, требованиями по безопасности, иными нормативными правовыми актами по обеспечению безопасности объектов защиты Учреждения, а также организационно-распорядительными документами по обеспечению информационной безопасности объектов защиты Учреждения.

План мероприятий утверждается главным врачом КГБУЗ КССМП и доводится до работников КГБУЗ КССМП в части, их касающейся.

Контроль за выполнением плана мероприятий осуществляется структурным подразделением, осуществляющим функции по обеспечению информационной безопасности в КГБУЗ КССМП. Специалисты структурного подразделения, осуществляющего функции по обеспечению информационной безопасности в КГБУЗ КССМП, ежегодно, должны готовить отчет о выполнении плана мероприятий, который представляется главному врачу КГБУЗ КССМП.

5.10.2. Осуществление внедрения мероприятий по обеспечению информационной безопасности объектов защиты Учреждения.

Осуществление внедрения (реализация) мероприятий по обеспечению информационной безопасности объектов защиты Учреждения является результатом выполнения плана мероприятий и осуществляется в соответствии с организационно-распорядительными документами по безопасности объектов защиты Учреждения.

В ходе реализации мероприятий по обеспечению информационной безопасности объектов защиты Учреждения должны приниматься организационные меры и (или) внедряться средства защиты информации, направленные на блокирование (нейтрализацию) угроз безопасности информации.

Результаты реализации мероприятий по обеспечению безопасности значимых объектов критической информационной инфраструктуры подлежат документированию в порядке, установленном действующим законодательством Российской Федерации и локальными правовыми актами Учреждения.

По завершению внедрения мероприятий по обеспечению информационной безопасности объектов защиты Учреждения, должен осуществляться контроль состояния информационной безопасности объектов защиты Учреждения.

В рамках контроля состояния информационной безопасности объектов защиты Учреждения должен осуществляться внутренний контроль организации работ по обеспечению информационной безопасности объектов защиты Учреждения и эффективности реализованных мероприятий.

В ходе проведения контроля проверяется выполнение требований действующего законодательства Российской Федерации, требований по безопасности, иных нормативных правовых актов и организационно-распорядительных документов в области обеспечения информационной безопасности объектов защиты Учреждения.

Контроль проводится комиссией, назначаемой приказом КГБУЗ КССМП. В состав комиссии включаются работники структурного подразделения, осуществляющего функции по обеспечению информационной безопасности, работники подразделений, эксплуатирующие объекты защиты Учреждения, и подразделений, обеспечивающих функционирование объектов защиты Учреждения.

Контроль состояния информационной безопасности объектов защиты КГБУЗ КССМП проводится не реже, чем раз в 3 года. Периодичность контроля определяется главным врачом КГБУЗ КССМП.

Для оценки эффективности принятых организационных и технических мер по обеспечению информационной безопасности объектов защиты КГБУЗ КССМП могут применяться средства контроля (анализа) защищенности.

Результаты контроля оформляются актом, который подписывается членами комиссии и утверждается главным врачом КГБУЗ КССМП.

В случае необходимости, главный врач КГБУЗ КССМП принимает решение о привлечении организаций к осуществлению мероприятий по контролю состояния информационной безопасности КГБУЗ КССМП (внешний аудит). При этом могут привлекаться исключительно организации, имеющие лицензии на соответствующий вид деятельности.

Замечания, выявленные по результатам внутреннего контроля или внешней оценки (внешнего аудита), подлежат устранению в порядке и сроки, устанавливаемые главным врачом КГБУЗ КССМП.

5.10.3. Повышение эффективности информационной безопасности объектов защиты КГБУЗ КССМП.

В рамках повышения эффективности безопасности объектов защиты КГБУЗ КССМП структурным подразделением, осуществляющим функции по обеспечению информационной безопасности, проводится анализ функционирования системы безопасности и состояния безопасности объектов защиты, по результатам которого разрабатываются предложения по развитию системы безопасности и меры по совершенствованию безопасности объектов защиты.

Анализ функционирования системы безопасности, а также разработка предложений по совершенствованию безопасности объектов защиты реализуются структурным подразделением, осуществляющим функции по обеспечению информационной безопасности, с участием подразделений (работников), эксплуатирующих объекты защиты, и подразделений (работников), обеспечивающих функционирование объектов защиты.

Предложения по совершенствованию безопасности объектов защиты представляются главному врачу КГБУЗ КССМП.

В соответствии с решением главного врача КГБУЗ КССМП предложения по совершенствованию безопасности объектов защиты включаются в план мероприятий, разрабатываемый в соответствии с п. 3.2.1 настоящей Политики.

5.10.4. Принятие организационных и технических мер для обеспечения информационной безопасности объектов защиты Учреждения.

Принятие организационных и технических мер по обеспечению безопасности объекта защиты осуществляется силами КГБУЗ КССМП и (или) лицом, привлекаемым в соответствии с законодательством Российской Федерации к проведению работ по обеспечению безопасности, в соответствии с техническим заданием на создание подсистемы безопасности объекта защиты.

При разработке организационных и технических мер по обеспечению безопасности объекта защиты учитывается его информационное взаимодействие с иными объектами, информационными системами, автоматизированными системами управления или информационно-телекоммуникационными сетями.

Разрабатываемые организационные и технические меры по обеспечению безопасности объекта защиты не должны оказывать негативного влияния на создание и функционирование данного объекта.

5.10.5. Установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения информационной безопасности объектов защиты Учреждения.

Установление параметров и характеристик программных и программно-аппаратных средств, применяемых для обеспечения информационной безопасности объектов защиты Учреждения, включает следующие этапы:

– определение требований к средству обеспечения ИБ: определение конкретных функций средства, необходимых для достижения целей по информационной безопасности объекта защиты, в соответствии с актуальными угрозами и рисками информационной безопасности, а также в соответствии с требованиями настоящей Политики;

– выбор средств обеспечения ИБ, соответствующих установленным требованиям к функционалу данных средств обеспечения ИБ;

– настройку параметров безопасности для каждого средства обеспечения ИБ, включая настройку, правил доступа к средству обеспечения ИБ, с целью его администрирования;

– установление параметров аутентификации, включая настройку методов аутентификации и авторизации;

– выбор и реализация способов безопасного информационного обмена аутентификационной информацией пользователя со средством обеспечения ИБ с использованием ИТС и хранения настоящей информации на устройствах;

– настройку мониторинга средства обеспечения ИБ для отслеживания событий безопасности и выявления потенциальных угроз, в части функциональных пределов средства обеспечения ИБ;

– настройку оповещения лиц, ответственных за управление (администрирование) подсистемой безопасности (системой защиты информации) объектов защиты Учреждения о событиях безопасности.

Установление параметров и характеристик средств обеспечения ИБ объектов защиты Учреждения должно учитывать требования к производительности объектов защиты, в отношении которых применяются данные средства обеспечения ИБ.

5.11. Создание СОИБ организует должностное лицо, ответственное за обеспечение информационной безопасности, в соответствии с Положением об ответственном за обеспечение информационной безопасности в КГБУЗ КССМП. Должностное лицо, ответственное за обеспечение информационной безопасности назначается приказом.

5.12. Мероприятия, направленные на создание СОИБ, реализует структурное подразделение КГБУЗ КССМП, осуществляющее функции по обеспечению информационной безопасности, в соответствии с Положением о структурном подразделении КГБУЗ КССМП, обеспечивающем информационную безопасность и указаниями ответственного за обеспечение информационной безопасности в КГБУЗ КССМП. Обязанности по обеспечению информационной безопасности возлагаются на структурное подразделение приказом.

6 ОТВЕТСТВЕННОСТЬ

Ответственность за правильность разработки, актуализацию и внедрение Политики информационной безопасности КГБУЗ КССМП несет заместитель главного врача по ОМР.

Работники Учреждения несут персональную ответственность за:

– соблюдение требований настоящей Политики информационной безопасности Учреждения;

– непредоставление непосредственному руководителю информации о случаях нарушения настоящей политики информационной безопасности, ставших ему известными.

7 ВНЕСЕНИЕ ИЗМЕНЕНИЙ

Внесение изменений в подлинник настоящего стандарта производит заместитель главного врача по ОМР совместно с менеджером, ответственным за систему менеджмента качества.

Предложения по внесению изменений в содержание настоящего стандарта может внести любой сотрудник. Предложения передаются заместителю главного врача по ОМР.

8 ХРАНЕНИЕ

Подлинник настоящего стандарта хранится в отделе системе менеджмента качества.

Срок хранения подлинника – до минования надобности.

Электронная версия утвержденного стандарта располагается на сетевых ресурсах КГБУЗ КССМП:

- X:\ДОКУМЕНТЫ КССМП\Стандарты учреждения

ВЕДОМОСТЬ ОБУЧЕНИЯ И ОЗНАКОМЛЕНИЯ С ПОРЯДКОМ

Структурное подразделение:

____

____

Обучение провел:

____

______________________________________**подпись:** _____________________

Фамилия, инициалы	Должность	Подпись	Дата