Политика управления информационной безопасностью на территории Центральной референтной лаборатории

На территории Центральной референтной лаборатории (ЦРЛ) осуществляют деятельность следующие организации: РГП на ПХВ «Национальный научный центр особо опасных инфекций имени М. Айкимбаева» (ННЦООИ), Алматинский филиал Национального референтного центра по ветеринарии (АФ НРЦВ) и Филиал РГП «Национальный центр биотехнологии» КН МОН РК в г. Алматы (АФ НЦБ). Высшее руководство данных организаций (далее Руководство) совместно разработали настоящую политику в области информационной безопасности. Основной миссией Центральной референтной лаборатории (ЦРЛ) является обеспечение защиты жизни и здоровья граждан Республики Казахстан от опасных и особо опасных инфекционных заболеваний человека и животных; референтное изучение инфекционных заболеваний и патогенов; хранение национальных коллекций штаммов возбудителей, а также научно-аналитическая и экспертно-диагностическая функции.

Осуществление указанных деятельностей связано с управлением информацией и данными, являющихся важными информационными активами организаций, работающих на территории ЦРЛ, и зависит от обеспечения информационной безопасности, под которой понимается обеспечение конфиденциальности, целостности и доступности чувствительной информации и данных.

Цель Политики

Политика управления информационной безопасностью ЦРЛ устанавливает цели, задачи и подходы в области информационной безопасности, которыми ЦРЛ руководствуется в своей деятельности.

Основными целями настоящей Политики управления информационной безопасностью являются:

- соответствие требованиям национального законодательства и существующих договоров;
- обеспечение непрерывности основных бизнес-процессов на территории ЦРЛ;
- минимизация рисков и возможного ущерба от нарушений в области информационной безопасности.

Система менеджмента информационной безопасности

Для достижения цели Руководство приняло решение разработать и внедрить систему менеджмента информационной безопасности, как часть интегрированной системы управления на территории ЦРЛ в соответствии с принципами, указанными в международном стандарте ISO/IEC 27001:2013. Система менеджмента информационной безопасности полностью учитывает требования национального и применимого международного законодательства.

Все информационные активы на территории ЦРЛ, подлежащие защите, категоризованы в соответствии с важностью для организаций. Категоризация информации документирована и утверждена Руководством в документированной процедуре «Идентификация, использование, хранение, передача, управление доступом и уничтожение чувствительной информации на территории ЦРЛ». Категоризация информационного актива проводится владельцем ресурса, хранящим или обрабатывающим его, для определения категории актива. На территории ЦРЛ подлежит управлению три категории информационных активов:

- Информация и данные, требующие повышенного уровня защиты;
- Информация и данные, которые требуют стандартного уровня защиты;
- Информация, которая не требует особой защиты.

Периодически категоризация пересматривается для поддержания актуальности её соответствия с категорией информационного актива.

Защита чувствительной информации на территории ЦРЛ основана на оценке рисков информационной безопасности, которая проводится в рамках Интегрированной системы менеджмента в соответствии с Методологией оценки и обработки рисков информационной безопасности . 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 управления рисками организации и критериям принятия рисков;
- избежание риска путём недопущения действий, могущих быть его причиной;
- передача рисков другой стороне (аутсорсинг, страхование и т.п.).

Принятые решения реализуются путем применения подходящих организационных, юридических или технических мер управления.

Область применения и границы

Настоящая Политика распространяется на всю информацию, которая является чувствительной для организаций, работающих на территории ЦРЛ, за исключением информации, попадающей под действие Закона Республики Казахстан «О государственных секретах» и иных ведомственных (отраслевых) перечней сведений, принятых министерствами и ведомствами согласно Постановлению Правительства Республики Казахстан от 14 марта 2000 года № 389 «Об утверждении Правил разработки ведомственных (отраслевых) перечней сведений, подлежащих засекречиванию».

Область применения Политики распространяется на все организации, работающих на территории ЦРЛ. Политика обязательна для применения для всех сотрудников и Руководства этих организаций, а также для пользователей их информационных активов.

Границы применения Политики менеджмента информационной безопасности - здание ЦРЛ, расположенное по адресу: Республика Казахстан, г. Алматы, ул. Жахангер, 14.

Цели системы менеджмента информационной безопасности

Стратегическими целями системы менеджмента информационной безопасности являются:

- обеспечение последовательного и систематического подхода к выявлению, анализу, оценке, воздействию, мониторингу рисков информационной безопасности и отчетности по ним;
- обеспечение того, что все роли и обязанности для лиц, имеющих воздействие на управление информационной безопасностью четко расписаны и доведены до соответствующих лиц;
- обеспечение того, что принятые решения выполняются в рамках утвержденных допустимых уровней риска и полностью обеспечивают защиту чувствительной информации;

- обеспечение гарантии, что внутренние средства управления существуют и работают эффективно и результативно, посредством внутреннего аудита, мониторинга, измерения, анализа и периодического пересмотра системы.

Уровень допустимости рисков

Руководство организаций, работающих на территории ЦРЛ, определяет следующий уровень **допустимого риска** информационной безопасности:

- приемлемыми считаются только риски от «низкого» до «умеренного» уровня, которые не несут существенную угрозу для жизни и здоровья людей, не ведут к нарушению применимого законодетельства и не приводят к урону репутации организаций, работающих на территории ЦРЛ (в соответствии с Методология оценки рисков информационной безопасности).

Руководство, осознавая свою ответственность за общее управление информационной безопасностью, декларирует свою приверженность к обеспечению соответствия применимым законодательным и договорным требованиям в области информационной безопасности и постоянному улучшению процесса управления информационной безопасностью на территории ЦРЛ.

Настоящая Политика должна пересматриваться не реже одного раза в год или в случае серьёзных изменений, влияющих на информационную безопасность на территории ЦРЛ и при необходимости, обновляться.

Генеральный директор РГП на ПХВ «Национальный научный центр особо опасных инфекций имени М. Айкимбаева», доктор медицинских наук	Ерубаев Токтасын Кенжеканович 05.11.2020г.
И.о.директора Алматинского филиала РГП на ПХВ «Национальный референтный центр по ветеринарии» КВК и Н МСХ РК,	Сулейменов Серик Толепбергенович 05.11.2020г.
И.о.директора Филиала РГП «Национальный центр биотехнологии» КН МОН РК в г. Алматы, кандидат биологических наук	Скиба Юрий Александрович 05.11.2020г.