Политика информационной безопасности

1. Общие положения и основные понятия

1. Настоящая Политика информационной безопасности ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области» определяет комплекс превентивных мер по защите информации, в том числе конфиденциальных данных, информационных процессов. На основе настоящей Политики строится управление информационной безопасностью ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области».
2. Настоящая Политика учитывает современное состояние и ближайшие перспективы развития вычислительной сети ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области», цели, задачи, эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее объектов информатизации.
3. Сопровождение серверов ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области» осуществляет Техническая служба.
4. Действие настоящей Политики распространяется на ведомства ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области» и территориальные подразделения, находящиеся в ведении ведомств, указанных в постановлении Правительства Республики Казахстан от 23 сентября 2014 года № 1005 «О некоторых вопросах Министерства здравоохранения и социального развития Республики Казахстан».
5. За нарушение положений настоящей политики пользователи привлекаются к дисциплинарной и иной ответственности, предусмотренной законодательством Республики Казахстан.
6. Основные понятия, используемые в настоящей Политике информационной безопасности Министерства (далее - Политика), определены законами Республики Казахстан от 11 января 2007 года «Об информатизации», от 21 мая 2013 года «О персональных данных и их защите», стандартах СТ РК 34.007-2002 «Информационная технология. Телекоммуникационные сети. Основные термины и определения», СТ РК 34.006-2002 «Информационная технология. Базы данных. Основные термины и определения», СТ РК 34.005-2002 «Информационная технология. Основные термины и определения», СТ РК 1699-2007 «Система контроля и управления доступом» и СТ РК 34.022-2006
«Защита информации Требования к проектированию, установке, наладке, эксплуатации и обеспечению безопасности информационных систем».

7. В настоящий Политике используется следующее основные понятие: служба технической поддержки (далее - Техническая служба) - юридическое лицо осуществляющее системно-техническое обслуживание программно-аппаратных средств, внедрение и (или) сопровождение информационных ресурсов и информационных систем;
3) информационная безопасность - процесс обеспечения защиты национальных информационных ресурсов, информационных систем, информационно-телекоммуникационной инфраструктуры от
4) неавторизованного доступа, использования, раскрытия, нарушения, изменения, прочтения, проверки, записи или уничтожения для обеспечения целостности, конфиденциальности и доступности информации, защита национального информационного пространства и систем распространения массовой информации от целенаправленного негативного информационного и организационного воздействия, могущего причинить ущерб национальным интересам Республики Казахстан;
5) информационная система (далее - ИС) - система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса;
6) электронные информационные ресурсы - информация, хранимая в электронном виде (информационные базы данных), содержащаяся в информационных системах;
7) информационные процессы - процессы создания, сбора, обработки, накопления, хранения, поиска, распространения и потребления информации;
8) информационная услуга - услуга по предоставлению пользователям информационных ресурсов;
9) конфиденциальность персональных данных - собственники и (или) операторы, а также третьи лица, получающие доступ к персональным данным ограниченного доступа, обеспечивают их конфиденциальность путем соблюдения требований не допускать их распространения без согласия субъекта или его законного представителя либо наличия иного законного основания, лица, которым стали известны персональные данные ограниченного доступа в связи с профессиональной, служебной необходимостью, а также трудовыми отношениями, обязаны обеспечивать их конфиденциальность;
10) вычислительная сеть (далее - ВС) - комплекс взаимосвязанных и согласованно функционирующих программных и аппаратных компонентов, предназначенный для решения задач обмена данными;

11) конфиденциальные электронные информационные ресурсы электронные информационные ресурсы, не содержащие государственных секретов, доступ

к которым ограничен в соответствии с законами Республики Казахстан или их собственником либо владельцем в случаях, предусмотренных законодательством Республики Казахстан;

несанкционированный доступ (далее - НСД) - получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к ней;

объект информатизации - электронные информационные ресурсы, информационные системы, информационные работы и электронные услуги;

разграничение доступа - порядок доступа лиц к техническим и программным средствам, секретной информации при ее обработке на средствах вычислительной техники в соответствии с заранее разработанными и утвержденными правилами;

электронно-вычислительная машина (компьютер) (далее - ЭВМ) - совокупность технических средств, основные функциональные устройства которой выполнены на электронных компонентах, создающая возможность проведение обработки информации и получения результата в необходимой форме.

субъект информатизации - государственные органы, физические и юридические лица, осуществляющие деятельность или вступающие в правоотношения в сфере информатизации на территории Республики Казахстан.

служебная тайна - сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан.

2. Потенциальные нарушители

8. Потенциальные нарушители подразделяются на внутренних и внешних. Внутренние нарушители - работники ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области», имеющие доступ к информации, составляющую коммерческую тайну и задействованные в технологии обработки, передачи и хранения информации.

9. К потенциальным внешним нарушителям относятся: бывшие работники Министерства; представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности (энерго-, во до-, теплоснабжения) ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области»;

посетители (приглашенные физические и (или) юридические лица, в том числе поставляющие технику, программное обеспечение, услуги).

10. Нарушениями настоящий Политики являются: несанкционированное использование программ, способных негативно повлиять на работоспособность ВС Министерства, снизить её производительность, а также затрудняющих работу ВС (сканеры сети, интенсивный широковещательный трафик); использование прав локальных администраторов на рабочих станциях пользователей, что дает возможность установки обычному пользователю неограниченного количества программ; нарушения работниками требований информационной безопасности Министерства и нормативных правовых актов.

3. Цели Политики

11. Главной целью, на достижение которой направлены все положения настоящий Политики, является надежное обеспечение информационной безопасности ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области», и как следствие недопущение нанесения материального, физического или иного ущерба в результате информационной деятельности.

12. Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния корпоративной вычислительной сети:

устойчивое функционирование ВС Министерства;

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

целостность и аутентичность информации, хранимой и обрабатываемой в ВС Министерства, и передаваемой по каналам связи.

4. Задачи Политики

13. Для достижения поставленных целей Департамент развития информатизации обеспечивает исполнение следующих задач:

защита от вмешательства посторонних лиц в процесс функционирования ВС ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области»;

разграничение доступа зарегистрированных пользователей к информации, а также к аппаратным, программно-аппаратным и программным средствам, включая средства криптографической защиты информации, используемым в ВС ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области»;

контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
защита системы от внедрения вредоносных кодов, включая компьютерные вирусы;
защита коммерческой тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;
обеспечение аутентификации пользователей, участвующих в информационном обмене;
своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;
создание механизма оперативного реагирования на угрозы информационной безопасности и негативные тенденции;
создание условий для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации.

5. Меры по информационной безопасности

14. В целях обеспечения защиты информационной безопасности, в том числе коммуникационных средств от несанкционированного доступа предусматривается следующие меры по информационной безопасности:
1) ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области»:
использование для производственных целей прикладного программного обеспечения, не входящего в состав базового комплекса; закрепление за каждым ЭВМ работника;
обеспечение прохождения инструктажа и дополнительного обучения, в том числе по нормам законодательства Республики Казахстан, предусмотренным в приложении к настоящей Политике пользователями корпоративной сети, в том числе вновь поступившими на работу;
проведение планового аудита информационной безопасности и в случае выявления в процессе аудита несоответствия требованиям информационной безопасности, внесение изменений и дополнений в настоящую Политику. Проведение планового аудита информационной безопасности является одним из основных методов проверки эффективности мер по защите информации. Результаты планового аудита служат основанием для пересмотра некоторых положений настоящий Политики и внесения в них необходимых корректировок;

закрепление в договорах обязательства поставщиков товаров, работ и услуг о неразглашении предоставленных им сведений, а также сведений, касающихся работы государственных информационных систем ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области» при заключении договоров, предмет которых затрагивает вопросы обеспечения информационной безопасности;
создание надежной системы охраны зданий и сооружений (видеонаблюдение, система контроля доступом), организация пропускного режима для предотвращения доступа посторонних лиц в здание;
осуществление закупа рабочих станций через официальных дилеров с завода производителя с документами, подтверждающими подлинность оборудования. Для защиты ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области» от нелицензионных программных обеспечений, внедрения и использования неучтенных программ
устанавливается базовый комплекс программного обеспечения на рабочих станциях пользователей. В базовый комплекс включается лицензионное программное обеспечение, необходимое для обеспечения работоспособности ЭВМ;
соблюдение требований настоящий Политики и иной нормативно-технической документации по обеспечению информационной безопасности утвержденной Министром здравоохранения и социального развития Республики Казахстан;
Технической службой:
отделение друг от друга основных и резервных телекоммуникационных сервисов ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области»;
включение и отключение серверного и телекоммуникационного оборудования;
обеспечение бесперебойного электропитания технических помещений, ежедневного удаленного мониторинга работы оборудования технических помещений, ограничение доступа к техническим помещениям и автоматическим выключателям электропитания;
сохранение важных резервных копий для восстановления данных при стихийных бедствиях и внештатных ситуациях;
принятие мер по защите при передаче ЭВМ на ремонт и в другие организации. В случае обнаружения фактов несанкционированного доступа к объектам информатизации или выявления потенциальной угрозы информационной безопасности, сотрудник, обнаруживший данный факт, немедленно ставит в известность системного администратора, своего

руководителя структурного подразделения и уполномоченное подразделение КНБ РК;
обеспечение систематического контроля возможности образования каналов утечки и оценки их опасности на границах контролируемой зоны (территории, помещения);
обеспечение технических средств защиты в ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области» в соответствии с используемыми каналами передачи информации;
отключение всех неиспользуемых в работе устройств ввода-вывода информации (WiFi, IR порты) на рабочих местах сотрудников, работающих с конфиденциальной информацией, удаление, не нужных для работы программных средств и данных с дисков. Дополнительные устройства обмена информацией используется только в качестве временного средства по согласованию с Управлением информационной безопасности Департамента развития информатизации.
защита ЭВМ пользователей от несанкционированного доступа в Министерстве, которая предусматривает следующие направления:
создание автоматизированных средств регистрации пользователей, система блокирования учетных записей и оповещения работников об угрозе или проникновении в ЭВМ;
определение организационных мер по предотвращению НСД, в том числе в случае утраты/компрометации паролей и выхода из строя ЭВМ;
использование лицензионного антивирусного программного обеспечения, специальных программ-анализаторов, осуществляющих постоянный контроль за возникновением отклонений в деятельности ВС Министерства, ежедневное проведение проверки на наличие возможных следов вирусной активности, а также входной контроль новых программ перед их использованием, регулярное обновление антивирусных программ. Антивирусные программы применяются для проверки рабочих станций, серверов Министерства, переносных носителей информации на наличие вредоносного кода;
тестирование перед вводом в эксплуатацию программных продуктов и аппаратных средств с целью проверки их работоспособности. Не пригодное к использованию программное обеспечение и аппаратные средства в эксплуатацию не принимаются;
осуществление контроля за незаконным подключением к корпоративной сети с применением программно-аппаратных средств и визуального регулярного осмотра технических помещений;
принятие мер, связанных с внедрением средств защиты, которые используются в случае стихийных бедствий • (пожаров, наводнений и

землетрясений), а также в различных внештатных ситуациях. Контроль за внештатными ситуациями производится путем внесения о них записей в журнал;
проведение ежедневного мониторинга состояния ВС, серверного оборудования, доступности каналов связи, в том числе с накоплением данных для анализа и отсылкой предупреждений при возникновении проблем. Мониторинг производиться удаленно с применением программно-аппаратных средств и визуально при обходе. Серверное оборудование имеет резервные диски горячей замены. Серверное и активно-сетевое оборудование имеет резервные мощности, позволяющие в случае внештатной ситуации восстановить работоспособность ВС в кратчайшие сроки;
соблюдение требований настоящей Политики и иной нормативно-технической документации по обеспечению информационной безопасности ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области»;
2) Пользователями:
копирование и передача служебной и иной защищаемой информации третьему лицу с письменного разрешения руководителя структурного подразделения ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области»;
передача информации содержащей сведения, составляющие государственные секреты только через подразделение по защите государственных секретов;
ограничение физического доступа к средствам отображения информации. На компьютере настраивается автоматическая блокировка экрана с паролем при неактивности пользователя более 5 минут;
передача ЭВМ в пользование другому работнику с письменного разрешения руководителя структурного подразделения ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области»;
соблюдение требований настоящий Политики и иной нормативно-технической документации по обеспечению информационной безопасности ГКП на ПХВ «Многопрофильная областная больница №2» Управления здравоохранения Акмолинской области».

6.Требования к серверным помещениям

15. Помещения для размещения серверного и активно-сетевого оборудования оснащаются:
1) системой контроля доступа. Контроль доступа в серверные помещения производится путем внесения в журнал записи о посещении серверного помещения;

2) системой видеонаблюдения;
3) системой кондиционирования, охлаждения. Температура в помещении должна поддерживаться в пределах 16-26 градусов Цельсия;
4) системой мониторинга температуры и электропитания;
5) системой охранной сигнализации;
6) системой пожарной сигнализации;
7) системой автоматического газового пожаротушения, а также ручными огнетушителями с углекислым газом;
8) металлической дверью с замком.
9) вводным электрощитом, расположенным внутри серверного помещения;
10) фальшполом огнеупорным и антистатическим, выдерживающим достаточную нагрузку. Укладка сигнальных линий связи производиться в специализированных подвесных металлических лотках. Электропитание прикладывается в фальшполе в специализированные металлические лотки. Электрические и сигнальные кабели располагается на расстояние не менее 50 сантиметров друг от друга или пересекаются под углом 90 градусов. Все серверные стойки и оборудование в них заземляются;
11) серверное и активное сетевое оборудование размещаются в серверные стойки с образованием «горячих» и «холодных» коридоров для оптимального охлаждения.