Политика информационной безопасности

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Политика информационной безопасности в Учреждении здравоохранения «Городская гинекологическая больница» (далее — Политика) определяет общие намерения по обеспечению конфиденциальности, целостности, подлинности, доступности и сохранности информации, в том числе и персональных данных.

2. Политика разработана с учетом нормативных правовых актов Республики Беларусь в области защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено:

- Концепция информационной безопасности Республики Беларусь, утвержденная постановлением Совета Безопасности от 18.03.2019 г.№ 1 «О Концепции информационной безопасности Республики Беларусь»;
- Закон Республики Беларусь от 18.06.1993 г. № 2435-XII «О здравоохранении»;
- Закон Республики Беларусь от 10.11.2008 г. № 455-З «Об информации, информатизации и защите информации»;
- Закон Республики Беларусь от 28.12.2009 г. №113-З «Об электронном документе и электронной цифровой подписи»;
- Указ Президента Республики Беларусь от 16.04.2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»;
- Постановление Совета Министров Республики Беларусь от 26.05.2009 г. № 673 «О некоторых мерах по реализации Закона Республики Беларусь «Об информации, информатизации и защите информации» и о признании утратившими силу некоторых постановлений Совета Министров Республики Беларусь»;
- Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 30.08.2013 г. № 62 «О некоторых вопросах технической криптографической защиты информации (в редакции приказа Оперативно– аналитического центра при Президенте Республики Беларусь от 11.10.2017 г. № 64);
- Приказ Министерства здравоохранения Республики Беларусь от 29.11.2019 г. № 1415 «О вопросах обеспечения информационной безопасности в здравоохранении»;
- а также международные нормативные правовые акты, ратифицированные в установленном порядке, в том числе международные технические нормативные акты, и технические нормативные правовые акты Республики Беларусь, содержащие положения по обеспечению безопасности информации.

3. Положения Политики служат основой для разработки локальных правовых актов, регламентирующих в Учреждении здравоохранения «Городская гинекологическая больница» (далее – Учреждение) вопросы защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено.

4. Ответственность за соблюдение информационной безопасности несет каждый сотрудник Учреждения, при этом первоочередной задачей является обеспечение безопасности всех активов Учреждения. Это значит, что информация должна быть защищена не менее надежно, чем любой другой основной актив Учреждения. Главные цели Учреждения не могут быть достигнуты без своевременного и полного обеспечения сотрудников информацией, необходимой им для выполнения своих служебных обязанностей.

5. В настоящей Политике под термином «сотрудник» понимаются все сотрудники Учреждения. На лиц, работающих в Учреждении по договорам гражданско-правового характера, в том числе прикомандированных, положения настоящей Политики распространяются в случае, если это обусловлено в таком договоре.

ГЛАВА 2
ЦЕЛИ И ПРИЧИНЫ ЗАЩИТЫ ИНФОРМАЦИИ

6. Целями и причинами защиты информации являются:

6.1. сохранение конфиденциальности информационных ресурсов;

6.2. обеспечение непрерывности доступа к информационным ресурсам Организации для поддержки бизнес деятельности;

6.3. защита целостности деловой информации с целью поддержания возможности Организации по оказанию услуг высокого качества и принятию эффективных управленческих решений.

ГЛАВА 3
НАЗНАЧЕНИЕ НАСТОЯЩЕЙ ПОЛИТИКИ

7. Повышение осведомленности пользователей в области рисков, связанных с информационными ресурсами Учреждения;

8. Определение степени ответственности и обязанностей сотрудников по обеспечению информационной безопасности в Учреждении.

9. Обеспечение регулярного контроля за соблюдением положений настоящей Политики и проведение периодических проверок соблюдения информационной безопасности с последующим представлением отчета по результатам указанной проверки руководителю Учреждения.

ГЛАВА 4
ОБЛАСТЬ ПРИМЕНЕНИЯ НАСТОЯЩЕЙ ПОЛИТИКИ

10. Требования настоящей Политики распространяются на всю информацию и ресурсы обработки информации Учреждения. Соблюдение настоящей Политики обязательно для всех сотрудников (как постоянных, так и временных). В договорах с третьими лицами, получающими доступ к информации Учреждения, должна быть оговорена обязанность третьего лица по соблюдению требований настоящей Политики.

11. Учреждению принадлежит на праве собственности (в том числе на праве интеллектуальной собственности) вся деловая информация и вычислительные ресурсы, приобретенные (полученные) и введенные в эксплуатацию в целях осуществления ею деятельности в соответствии с действующим законодательством. Указанное право собственности распространяется на голосовую и факсимильную связь, осуществляемую с использованием оборудования Учреждения, лицензионное и разработанное программное обеспечение, содержание ящиков электронной почты, бумажные и электронные документы всех функциональных подразделений и персонала Учреждения.

ГЛАВА 5
ПЕРЕЧЕНЬ ИФОРМАЦИОННЫХ СИСТЕМ И СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ

12. В Учреждения используются информационная система, в которой обрабатывается информация о частной жизни физического лица и персональные данные, иная информация, составляющая охраняемую законом тайну физического лица, распространение и (или) предоставление которой ограничено, отнесенная к соответствующему классу 3-фл типовых информационных систем.

ГЛАВА 6
СВЕДЕНИЯ О ПОДРАЗДЕЛЕНИИ ЗАЩИТЫ ИНФОРМАЦИИ

13. В Учреждении защитой информации, в том числе и персональных данных, занимаются назначенные ответственные лица.

14. Основными задачами ответственных лиц по защите информации являются:

14.1. разработка и внедрение организационных и технических мероприятий по комплексной защите информации Учреждения;

14.2. сохранение конфиденциальности документированной информации;

14.3. разработка проектов перспективных и текущих планов работ по комплексной защите информации Учреждения, составление отчетов об их выполнении;

14.4. разработка технических средств контроля по комплексной защите информации Учреждения;

14.5. формирование целей и задач работы по созданию безопасных информационных технологий, отвечающих требованиям комплексной защиты информации Учреждения;

14.6. обеспечение контроля за соблюдением нормативных требований по надежной защите информации;

14.7. обеспечение комплексного использования технических средств, методов и организационных мероприятий для защиты информации Учреждения.

ГЛАВА 7
ОБЩИЕ ПОЛОЖЕНИЯ КОНТРОЛЯ ДОСТУПА К ИНФОРМАЦИОННЫМ СИСТЕМАМ

15. Все работы в пределах Учреждения выполняются в соответствии с официальными должностными обязанностями только на компьютерах, разрешенных к использованию в Учреждении.

16. Внос в здания и помещения Учреждения личных портативных компьютеров и внешних носителей информации (диски, флэш-карты и т.п.), а также вынос их за пределы Учреждения производится только при согласовании с ответственными лицами по защите информации.

17. Все конфиденциальные данные, составляющие коммерческую тайну Учреждения и хранящиеся на жестких дисках портативных компьютеров, должны быть зашифрованы. Все портативные компьютеры Учреждения должны быть оснащены программным обеспечением по шифрованию жесткого диска. Руководители подразделений должны периодически пересматривать права доступа своих сотрудников и других пользователей к соответствующим информационным ресурсам.

18. В целях обеспечения санкционированного доступа к информационному ресурсу, любой вход в систему должен осуществляться с использованием уникального имени пользователя и пароля.

19. Пользователи должны руководствоваться рекомендациями по защите своего пароля на этапе его выбора и последующего использования. Запрещается сообщать свой пароль другим лицам или предоставлять свою учетную запись другим, в том числе членам своей семьи и близким, если работа выполняется дома.

20. В процессе своей работы сотрудники обязаны постоянно использовать режим «Экранной заставки» с парольной защитой. Рекомендуется устанавливать максимальное время «простоя» компьютера до появления экранной заставки не дольше 15 минут.

ГЛАВА 8

ДОСТУП ТРЕТЬИХ ЛИЦ К ИНФОРМАЦИОННЫМ СИСТЕМАМ УЧРЕЖДЕНИЯ

21. Каждый сотрудник обязан немедленно уведомить ответственных по защите информации обо всех случаях предоставления доступа третьим лицам к ресурсам корпоративной сети.

22. Доступ третьих лиц к информационным системам Учреждения должен быть обусловлен производственной необходимостью. В связи с этим, порядок доступа к информационным ресурсам Учреждения должен быть четко определен, контролируем и защищен.

ГЛАВА 9
УДАЛЕННЫЙ ДОСТУП

23. Пользователи получают право удаленного доступа к информационным ресурсам Учреждения с учетом их взаимоотношений с Учреждением.

24. Сотрудникам, использующим в работе персональные компьютеры Учреждения, может быть предоставлен удаленный доступ к сетевым ресурсам Учреждения в соответствии с правами в информационной системе Учреждения.

25. Сотрудникам, работающим за пределами Учреждения с использованием компьютера, не принадлежащего Учреждению, запрещено копирование данных на компьютер, с которого осуществляется удаленный доступ.

26. Сотрудники и третьи лица, имеющие право удаленного доступа к информационным ресурсам Учреждения, должны соблюдать требование, исключающее одновременное подключение их компьютера к сети Учреждения и к каким-либо другим сетям, не принадлежащим Учреждению.

27. Все компьютеры, подключаемые посредством удаленного доступа к информационной сети Учреждения, должны иметь программное обеспечение антивирусной защиты, имеющее последние обновления.

ГЛАВА 10
ДОСТУП К СЕТИ ИНТЕРНЕТ

28. Доступ к сети Интернет обеспечивается только в производственных целях и не может использоваться для незаконной деятельности.

29. Рекомендованные правила:

29.1. сотрудникам Учреждения разрешается использовать сеть Интернет только в служебных целях;

29.2. запрещается посещение любого сайта в сети Интернет, который считается оскорбительным для общественного мнения или содержит информацию сексуального характера, пропаганду расовой

ненависти, комментарии по поводу различия/превосходства полов, дискредитирующие заявления или иные материалы с оскорбительными высказываниями по поводу чьего-либо возраста, сексуальной ориентации, религиозных или политических убеждений, национального происхождения или недееспособности;

29.3. работа сотрудников Учреждения с Интернет-ресурсами допускается только режимом просмотра информации, исключая возможность передачи информации Учреждения в сеть Интернет;

29.4. сотрудники Учреждения перед открытием или распространением файлов, полученных через сеть Интернет, должны проверить их на наличие вирусов;

29.5. запрещен доступ в Интернет через сеть Учреждения для всех лиц, не являющихся сотрудниками Учреждения, включая членов семьи сотрудников Учреждения.

29. Ответственные лица по защите информации имеют право контролировать содержание всего потока информации, проходящей через канал связи к сети Интернет в обоих направлениях.

ГЛАВА 11
ЗАЩИТА ОБОРУДОВАНИЯ

30. Сотрудники должны постоянно помнить о необходимости обеспечения физической безопасности оборудования, на котором хранятся информация Учреждения.

31. Сотрудникам запрещено самостоятельно изменять конфигурацию аппаратного и программного обеспечения. Все изменения производят ответственные по защите информации.

ГЛАВА 12
АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

32. Все компьютерное оборудование (серверы, персональные компьютеры), периферийное оборудование (например, принтеры и сканеры), аксессуары (манипуляторы типа «мышь», дисководы для CD-дисков), коммуникационное оборудование (например, сетевые адаптеры и коммутаторы), для целей настоящей Политики вместе именуются «компьютерное оборудование». Компьютерное оборудование, предоставленное Учреждением, является ее собственностью и предназначено для использования исключительно в производственных целях.

33. Пользователи персональных компьютеров, содержащих информацию, составляющую коммерческую тайну Учреждения, обязаны обеспечить их хранение в физически защищенных помещениях.

34. Все компьютеры должны защищаться паролем при загрузке системы, активации по горячей клавиши и после выхода из режима «Экранной заставки». Для установки режимов защиты пользователь

должен обратиться в службу технической поддержки. Данные не должны быть скомпрометированы в случае халатности или небрежности приведшей к потере оборудования. Перед утилизацией все компоненты оборудования, в состав которых входят носители данных (включая жесткие диски), необходимо проверять, чтобы убедиться в отсутствии на них конфиденциальных данных и лицензионных продуктов. Должна выполняться процедура форматирования носителей информации, исключающая возможность восстановления данных.

35. Порты передачи данных, в том числе FD и CD дисководы в стационарных компьютерах сотрудников Организации блокируются, за исключением тех случаев, когда сотрудником получено разрешение на запись информации у специалиста отдела по защите информации.

ГЛАВА 13
ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

36. Все программное обеспечение, установленное на предоставленном Учреждением компьютерном оборудовании, является собственностью Учреждения и должно использоваться исключительно в производственных целях.

37. Сотрудникам запрещается устанавливать на предоставленном в пользование компьютерном оборудовании нестандартное, нелицензионное программное обеспечение или программное обеспечение, не имеющее отношения к их производственной деятельности. Если в ходе выполнения технического обслуживания будет обнаружено не разрешенное к установке программное обеспечение, оно будет удалено, а сообщение о нарушении будет направлено непосредственному руководителю сотрудника и ответственным лицам по защите информации.

38. На всех портативных компьютерах должны быть установлены программы, необходимые для обеспечения защиты информации:

39.1. персональный межсетевой экран;

39.2. антивирусное программное обеспечение;

39.3. программное обеспечение шифрования жестких дисков;

39.4. программное обеспечение шифрования почтовых сообщений.

39. Все компьютеры, подключенные к сети Учреждения, должны быть оснащены системой антивирусной защиты, утвержденной ответственными лицами по защите информации.

40. Сотрудники Учреждения не должны:

40.1. блокировать антивирусное программное обеспечение;

40.2. устанавливать другое антивирусное программное обеспечение;

40.3. изменять настройки и конфигурацию антивирусного программного обеспечения.

ГЛАВА 14
РЕКОМЕНДУЕМЫЕ ПРАВИЛА ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ ПОЧТОЙ

41. Электронные сообщения (удаленные или не удаленные) могут быть доступны или получены государственными органами для их использования в качестве доказательств в процессе судебного разбирательства. Поэтому содержание электронных сообщений должно строго соответствовать стандартам Учреждения в области деловой этики.

42. Использование электронной почты в личных целях допускается в случаях, когда получение/отправка сообщения не мешает работе других пользователей и не препятствует бизнес деятельности.

43. Сотрудникам запрещается направлять партнерам конфиденциальную информацию Учреждения по электронной почте без использования систем шифрования. Строго конфиденциальная информация Учреждения, ни при каких обстоятельствах, не подлежит пересылке третьим лицам по электронной почте.

44. Сотрудникам Учреждения запрещается использовать личные почтовые ящики электронной почты для осуществления деятельности Учреждения.

45. Использование сотрудниками Учреждения личных почтовых ящиков электронной почты осуществляется только при согласовании с ответственными лицами по защите информации при условии применения механизмов шифрования.

46. Сотрудники Учреждения для обмена документами с бизнес партнерами должны использовать только свой официальный адрес электронной почты.

47. Сообщения, пересылаемые по электронной почте, имеют тот же статус, что и письма, и факсимильные сообщения. Электронные сообщения подлежат такому же утверждению и хранению, что и прочие средства письменных коммуникаций.

48. В целях предотвращения ошибок при отправке сообщений пользователи перед отправкой должны внимательно проверить правильность написания имен и адресов получателей. В случае получения сообщения лицом, вниманию которого это сообщение не предназначается, такое сообщение необходимо переправить непосредственному получателю. Если полученная таким образом информация носит конфиденциальный характер, об этом следует незамедлительно проинформировать специалистов отдела по защите информации.

49. Ниже перечислены недопустимые действия и случаи использования электронной почты:

50.1. рассылка сообщений личного характера, использующих значительные ресурсы электронной почты;

50.2. групповая рассылка всем пользователям Учреждения сообщений/писем;

50.3. подписка на рассылку, участие в дискуссиях и подобные услуги, использующие значительные ресурсы электронной почты в личных целях;

50.4. поиск и чтение сообщений, направленных другим лицам (независимо от способа их хранения);

50.5. пересылка любых материалов, как сообщений, так и приложений, содержание которых является противозаконным, непристойным, злонамеренным, оскорбительным, угрожающим, клеветническим, злобным или способствует поведению, которое может рассматриваться как уголовное преступление или административный проступок либо приводит к возникновению гражданско-правовой ответственности, беспорядков или противоречит стандартам Учреждения в области этики.

51. Вложения, отправляемые вместе с сообщениями, следует использовать с должной осторожностью. Во вложениях всегда должна указываться дата их подготовки, и они должны оформляться в соответствии с установленными в Учреждения процедурами документооборота.

52. Пересылка значительных объемов данных в одном сообщении может отрицательно повлиять на общий уровень доступности сетевой инфраструктуры Учреждения для других пользователей.

ГЛАВА 15
СООБЩЕНИЯ ОБ ИНЦИДЕНТАХ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, РЕАГИРОВАНИЕ И ОТЧЕТНОСТЬ

53. Все пользователи должны быть осведомлены о своей обязанности сообщать об известных или подозреваемых ими нарушениях информационной безопасности, а также должны быть проинформированы о том, что ни при каких обстоятельствах они не должны пытаться использовать ставшие им известными слабые стороны системы безопасности.

54. Пользователи должны знать способы информирования об известных или предполагаемых случаях нарушения информационной безопасности с использованием телефонной связи, электронной почты и других методов. Необходимо обеспечить контроль и учет сообщений об инцидентах и принятие соответствующих мер.

55. Если имеется подозрение или выявлено наличие вирусов или иных разрушительных компьютерных кодов, то сразу после их обнаружения сотрудник обязан:

55.1. проинформировать специалистов по защите информации;

55.2. не пользоваться и не выключать зараженный компьютер;

55.3. не подсоединять этот компьютер к компьютерной сети Учреждения до тех пор, пока на нем не будет произведено удаление обнаруженного вируса и полное антивирусное сканирование специалистами отдела по защите информации.

ГЛАВА 16
ПОМЕЩЕНИЯ С ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

56. Конфиденциальные встречи (заседания) должны проходить только в защищенных техническими средствами информационной безопасности помещениях.

57. Перечень помещений с техническими средствами информационной безопасности утверждается руководителем Учреждения.

58. Участникам заседаний запрещается входить в помещения с записывающей аудио/видео аппаратурой, фотоаппаратами, радиотелефонами и мобильными телефонами без предварительного согласования со специалистами отдела по защите информации.

59. Доступ участников конфиденциального заседания в помещение для его проведения осуществляется на основании утвержденного перечня, контроль за которым ведет лицо, отвечающее за организацию встречи.

ГЛАВА 17
УПРАВЛЕНИЕ СЕТЬЮ

60. Уполномоченные специалисты по защите информации контролируют содержание всех потоков данных, проходящих через сеть Учреждения.

61. Сотрудникам Учреждения запрещается:

61.1. нарушать информационную безопасность и работу сети Учреждения;

61.2. сканировать систему безопасности;

61.3. контролировать работу сети с перехватом данных;

61.4. получать доступ к компьютеру, сети или учетной записи в обход системы идентификации пользователя или безопасности;

61.5. использовать любые программы, команды или передавать сообщения с целью вмешаться в работу или отключить пользователя устройства;

61.6. передавать информацию о сотрудниках или списки сотрудников Учреждения посторонним лицам;

61.7.создавать, обновлять или распространять компьютерные вирусы и прочие разрушительное программное обеспечение.

ГЛАВА 18
ЗАЩИТА И СОХРАННОСТЬ ДАННЫХ

62. Ответственность за сохранность данных на стационарных х персональных компьютерах лежит на пользователях. Специалисты по защите информации обязаны оказывать пользователям содействие в проведении резервного копирования данных на соответствующие носители.

63. Необходимо регулярно делать резервные копии всех основных служебных данных и программного обеспечения.

64. Только специалисты отдела по защите информации на основании заявок руководителей подразделений могут создавать и удалять совместно используемые сетевые ресурсы и папки общего пользования, а также управлять полномочиями доступа к ним.

65. Сотрудники имеют право создавать, модифицировать и удалять файлы в совместно используемых сетевых ресурсах только на тех участках, которые выделены лично для них, для их рабочих групп или к которым они имеют разрешенный доступ.

66. Все заявки на проведение технического обслуживания компьютеров должны направляться в отдел по защите информации.

ГЛАВА 19
РАБОТА С КРИПТОГРАФИЧЕСКИМИ СИСТЕМАМИ

67. К работе с криптографическими системами допускаются только сотрудники Учреждения, имеющие соответствующее разрешение от директора Учреждения.

68. Секретные ключи электронно-цифровых подписей и шифрования должны храниться в сейфах под ответственностью уполномоченных лиц. Доступ неуполномоченных лиц к носителям секретных ключей и шифрования должен быть исключен.

69. Категорически запрещается:

69.1. выводить секретные ключи и шифрования на дисплей компьютера или принтер;

69.2. устанавливать в дисковод компьютера носитель секретных ключей и шифрования в непредусмотренных режимах функционирования;

69.3. записывать на носитель секретных ключей и шифрования постороннюю информацию.

70. При компрометации секретных ключей, шифрования и прочей электронной информации Учреждением принимаются меры для прекращения любых операций с использованием этих ключей и прочей информации; принимаются меры для смены ключей и шифрования, паролей. По факту компрометации организуется служебное

расследование, результаты которого отражаются в акте и доводятся до сведения руководителя Учреждения.

ГЛАВА 20
РАЗРАБОТКА СИСТЕМ И УПРАВЛЕНИЕ ВНЕСЕНИЕМ ИЗМЕНЕНИЙ

71. Все операционные процедуры и процедуры внесения изменений в информационные системы и сервисы должны быть документированы и согласованны с начальником отдела по защите информации.