Министерство здравоохранения
Республики Беларусь
Учреждение образования
«Гродненский государственный
медицинский университет»

УТВЕРЖДАЮ
Ректор университета,
профессор
_____ И.Г.Жук
26.11.2024

ПОЛОЖЕНИЕ

26.11.2024 № 01-04/13
г. Гродно

О защите информации

ГЛАВА 1
ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее положение о защите информации (далее – положение) в учреждении образования «Гродненский государственный медицинский университет» (далее – университет) устанавливает основные требования, связанные с доступом к информации, защитой от нарушения конфиденциальности, ненадлежащим использованием, нарушением целостности и резервным копированием данных.

2. Положение разработано в соответствии с:

2.1. СТБ ISO/IEC 27002-2012 «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности» (далее – СТБ 27002);

2.2. СТ РК ISO/IEC 27002-2015 «Информационная технология. Методы и средства обеспечения безопасности. Свод правил по средствам управления защитой информации»;

2.3. ISO/IEC 27003:2017 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство» (Information technology – Security techniques – Information security management systems – Guidance);

2.4. Законом Республики Беларусь от 10.11.2008 № 455-З «Об информации, информатизации и защите информации»;

2.5. Законом Республики Беларусь от 7.05.2021 № 99-З «О защите персональных данных»;

2.6. Письмом Министерства здравоохранения Республики Беларусь от 12.08.2016 № 1-1-9/2157 «Об усилении мер в области информационной безопасности»;

2.7. Техническим регламентом Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность»

(ТР 2013/027/BY), утвержденным постановлением Совета Министров Республики Беларусь от 15.05.2013 № 375 (в редакции постановления Совета Министров Республики Беларусь 12.03.2020 № 145);

2.8. Приказом Оперативно-аналитического центра при Президенте Республики Беларусь 20.02.2020 № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9.12.2019 № 449».

3. Признать утратившим силу положение ректора университета от 27.07.2018 №01-02/10 «О защите информации».

ГЛАВА 2
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ СЕТЯХ, ПОДКЛЮЧЕННЫХ К СЕТИ ИНТЕРНЕТ

4. Пользователями локальной вычислительной сети университета являются работники, получившие авторизованный доступ.

5. Администрирование локальной вычислительной сети университета выполняют администраторы системные отдела образовательных информационных технологий и научно-медицинской информации (далее – ООИТ и НМИ) университета.

6. Администраторы системные обязаны:

6.1. предоставлять авторизованный доступ работникам университета к локальной сети университета и сервисам сети Интернет на основании заключенного договора на оказание услуг доступа к локальной вычислительной сети и информационным ресурсам;

6.2. предотвращать доступ неавторизованных пользователей и разграничивать доступ зарегистрированных пользователей к ресурсам сети Интернет;

6.3. обеспечить контроль использования работниками ресурсов сети Интернет;

6.4. определять порядок применения средств защиты информации, установленных в локальной вычислительной сети;

6.5. обеспечить идентификацию абонентских устройств в локальной сети;

6.6. обеспечить межсетевое экранирование с использованием собственных возможностей и (или) возможностей уполномоченных поставщиков интернет-услуг;

6.7. осуществлять сбор и хранение данных авторизации и статистики использования сети Интернет-пользователями в течение 1 года;

6.8. применять криптографические протоколы для защиты данных авторизации при работе с сервисами сети Интернет.

7. Работники университета несут персональную ответственность за информацию, получаемую и передаваемую посредством сети Интернет.

8. Приказом ректора университета из работников ООИТ и НМИ и (или) отдела безопасности назначается ответственный за обязательное наличие и использование постоянно обновляемого сертифицированного антивирусного

программного обеспечения, а также межсетевых экранов; проведение постоянной работы по обновлению баз данных средств антивирусной защиты информации; по обнаружению и обезвреживанию вредоносных программ.

9. Руководителем структурного подразделения университета назначается ответственный за обновление баз данных антивирусного программного обеспечения на всех оборудованных антивирусом компьютерах структурного подразделения.

ГЛАВА 3
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ, РАСПОЛОЖЕННОЙ НА ОФИЦИАЛЬНОМ САЙТЕ УНИВЕРСИТЕТА

10. Официальный сайт университета http://www.grsmu.by (далее – сайт) обеспечивает официальное представление информации об университете в сети Интернет с целью развития учебно-методических, научных связей, способствующих расширению образовательных и медицинских услуг, оперативного ознакомления пользователей с различными аспектами его деятельности, повышения эффективности взаимодействия подразделений университета с целевой аудиторией.

11. Контент сайта расположен на сервере университета.

12. Посетителем сайта может быть любое лицо, имеющее технические возможности выхода в Интернет.

13. Вся информация, размещаемая на сайте, предназначена для открытого общего доступа.

14. Доступом к администрированию сайта обладают: специалист по контенту отдела по связям с общественностью и маркетингу (далее – ОСО и М), специалист по работе с социальными сетями ОСО и М, начальник ОСО и М, начальник ООИТ и НМИ и инженеры-программисты ООИТ и НМИ.

15. Для каждого администратора сайта ООИТ и НМИ создает отдельную учетную запись с персональным логином и паролем. Персональные данные учетных записей администраторов сайта должны храниться в безопасности и не передаваться другим работникам или третьим лицам.

16. Работу по информационному наполнению разделов сайта осуществляет специалист по контенту или замещающий его работник, назначенный распоряжением начальника ОСО и М работник.

17. В случае необходимости начальник ООИТ и НМИ может назначать модераторов определенных разделов сайта из числа работников университета, с созданием персональных учетных записей для модерирования. Функциональные обязанности модераторов согласуются с начальником ОСО и М и специалистом по контенту ОСО и М, проводится обязательное обучение по модерированию разделов сайта.

18. Необходимые организационно – технические мероприятия для функционирования сайта в сети осуществляют работники ООИТ и НМИ.

19. Непосредственный контроль над работой сайта и информационным наполнением его разделов осуществляет специалист по контенту ОСО и М.

20. Общая координация работ по развитию сайта и контроль выполнения обязанностей лицами, участвующими в процессах информационного наполнения, актуализации и программно-технического сопровождения сайта, возлагается на первого проректора и проректора по идеологической и воспитательной работе.

21. Ответственность должностных лиц.

21.1. Ответственность за недостоверное или некачественное предоставление информации для размещения на сайте несет руководитель соответствующего структурного подразделения университета.

21.2. Ответственность за своевременное предоставление информации для размещения на сайте несут ответственные работники структурных подразделений согласно положению об официальных корпоративных интернет-ресурсах университета от 20.04.2023 № 01-02/13.

21.3. Ответственность за содержание информации, её своевременную актуализацию и удаление несут руководители соответствующих структурных подразделений.

21.4. Ответственность за текущее сопровождение сайта несет специалист по контенту ОСО и М, который обеспечивает своевременность размещения предоставляемой информации (в течение 3-х рабочих дней), назначенные начальником ООИТ и НМИ модераторы (при необходимости), работники ООИТ и НМИ, ответственные за выполнение необходимых программно-технических мероприятий по обеспечению целостности и доступности информационных ресурсов.

21.5. Ответственность за работоспособность сайта, реализацию концептуальных программно-технических решений несет начальник ООИТ и НМИ.

ГЛАВА 4
ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ РАСПОЛОЖЕННОЙ НА СЕРВЕРЕ УНИВЕРСИТЕТА

22. Серверное помещение оборудовано охранной сигнализацией и находится под охраной Ленинского отдела (г. Гродно) Департамента охраны Министерства внутренних дел Республики Беларусь.

23. Снятие помещения с охраны и последующая постановка на охрану производится ответственными лицами ООИТ и НМИ.

24. Администрирование серверов производится администраторами системными. Администрирование установленного программного обеспечения осуществляется инженерами-программистами ООИТ и НМИ.

25. Пользовательским доступом к информации, расположенной на сервере, обладают авторизированные пользователи (по направлению деятельности).

26. Администраторы системные и инженеры-программисты ООИТ и НМИ несут ответственность за:

26.1. доступ к активам сервера;

26.2. обязательное обеспечение резервного копирования объектов (файлы, базы данных, образы систем, дистрибутивы, исходные коды программных средств) с целью восстановления их в случае сбоя или уничтожения на отдельный сервер (сетевое хранилище), не имеющий выход в сеть Интернет;

26.3. восстановление работоспособности программного обеспечения в случае сбоя или уничтожения отдельных и/или всех серверов (хранилищ) и целостность баз данных из резервных копий в случае возникновения внештатной ситуации, вызвавшей нарушение работоспособности информационных систем университета;

26.4. наличие на сервере только той информации и тех программ, которые необходимы работникам университета для повседневной деятельности;

26.5. мониторинг состояния серверов и журнала активностей на сервере с целью выявления потенциальных угроз.

ГЛАВА 5
ОБЕСПЕЧЕНИЕ ДОКУМЕНТООБОРОТА ПОСРЕДСТВОМ ЭЛЕКТРОННОЙ ПОЧТЫ

27. Пользователями электронной почты университета являются работники, получившие авторизованный доступ.

Предоставление почтового ящика, перечень решаемых задач и условия использования определены в Положении об использовании корпоративной электронной почты, утвержденном приказом ректора университета от 01.08.2022 № 346.

28. Ответственность за создание учетных записей и их актуальность несут руководители структурных подразделений.

29. Ответственность за информацию, передаваемую посредством электронной почты, несут пользователи электронной почты.

ГЛАВА 6
РАБОТА С ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ

30. Прикладное программное обеспечение:

30.1. прикладное программное обеспечение устанавливается на клиентские места;

30.2. пользователями прикладного программного обеспечения являются работники университета;

30.3. работники университета несут персональную ответственность за информацию, создаваемую и обрабатываемую при помощи прикладного программного обеспечения, а также за ее распространение и хранение на локальных рабочих местах.

31. Специализированное программное обеспечение: