|  |  |
| --- | --- |
|  | **ФГБОУ ВО ВГМУ им. Н.Н. Бурденко Минздрава России** |

**ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ № 2  
30.03.2022**

**Уважаемые сотрудники структурных подразделений!**

Доводим краткую информацию о выполнении требований по информационной безопасности и защите персональных данных в ВГМУ им. Н.Н. Бурденко, реализуемых в рамках Приказа ректора № 194 от 22.03.2022 г.

* ***Информационная безопасность*** *—**практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.*
* ***Персональные данные*** *- любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных);*

**Меры, принятые в ВГМУ по защите информации:**

1. Запрещено использование личных съёмных машинных носителей информации (Флэш-накопители, внешние жёсткие диски, карты памяти), если они не прошли проверку специалистами по защите информации и не учтены в соответствующем журнале.
2. Служебные съёмные машинные носители информации должны храниться на рабочем месте, не имеющее свободного доступа и с ведением журнала об использовании данных носителей информации.
3. Не реже, чем 2 раза в месяц необходимо сдавать съёмные машинные носители информации в УИТ для проведения аудита данного оборудования (*график поверки будет выслан позже).*
4. Запрещено использование для работы с данными информационной инфраструктуры вуза, и подключение (сопряжение) **ЛИЧНОЙ** вычислительной техники (персональных компьютеров, ноутбуков, планшетов, смартфонов), печатной техники, модемов.

*Примечание – всё оборудование, которое не стоит на балансовом учёте вуза, не может быть использовано для работы с данными (документы, файлы, журналы) вуза.*

1. Ограничено использование иностранных ВКС платформах (Skype, Zoom, Discord, Teams и т.д.) для онлайн-мероприятий (конференции, занятия, олимпиады, совещания)
2. Запрещено использование иностранных сервисов, социальный сетей и мессенджеров **для сбора защищаемой информации, и работы с ней** (все сервисы Google и Mozilla, в том числе браузеры, WhatsApp, Viber, Twitter, Instagram, Facebook и т.д.).
3. Запрещено использование программ для удалённого доступа (AnyDesk, TeamViewer) по средствам сети Интернет (запрещено подключаться к рабочим местам из дома).

***Примечания.***

1. ***Удалённый доступ разрешён ТОЛЬКО по сертифицированным каналам связи и ТОЛЬКО при личном контроле IT-специалистов.***
2. ***Работа сотрудников университета системой «Тандем. Университет» продолжится в штатном режиме.***
3. Запрещена загрузка аудио- и видео-контента, интерфейсов взаимодействия и других материалов, со сторонних ресурсов на официальных сайтах вуза.
4. Запрещено пересылать данные (служебную информацию) на почтовые адреса, которые не относятся к российским доменам: com; .us; .uk; .net и другие домены стран Евросоюза.
5. Создан адрес электронной почты **SPAM@VRNGMU.RU**, на который необходимо пересылать любые подозрительные письма, которые пришли сотрудникам вуза.
6. Запрещён доступ к серверам компании Microsoft, а также обновления программных продуктов данной компании.
7. Запрещено использование программного обеспечения, которое не относится к рабочему процессу.
8. Ограничено использование Wi-Fi роутеров (будут отключены Wi-Fi сети, используемые для передачи, хранения и обработки персональных данных).
9. Произведена смена всех паролей Администратора на серверном, сетевом и пользовательском оборудовании.
10. Используемый в ВГМУ антивирус имеет действующий сертификат соответствия требованиям защиты информации ФСТЭК.

**ОТВЕТСТВЕННОСТЬ**

**Нарушение норм защиты информации –** дисциплинарная (замечание, выговор, увольнение), гражданско-правовая (возмещение морального вреда и убытков), административная (от 2 тысяч до 18 миллионов рублей) и уголовная (от штрафа 100 тысяч рублей до лишения свободы сроком до 5 лет) ответственность.

**ПРИМЕЧАНИЕ**

Об иных дополнительных мерах по информационной безопасности и защите персональных данных, вводимых в ВГМУ им. Н.Н.Бурденко, сотрудники подразделений будут оповещены дополнительно по средствам рассылки на служебные адреса электронных почтовых ящиков за 72 часа до введения этих мер.

***Приложение: Приказа ректора № 194 от 22.03.2022г***

|  |  |
| --- | --- |
|  |  |

**Контактная информация**

|  |  |
| --- | --- |
| **Проректор по цифровой трансформации**  Чопоров Олег Николаевич,  доктор технических наук , профессор  [onchoporov@vrngmu.ru](mailto:onchoporov@vrngmu.ru)  Раб.8 (473) 210-49-716 (239)  Моб.8 (903) 653-39-07 | **Зам. начальника УИТ по общим вопросам –**  **специалист по защите информации**  Харин Александр Валерьевич  [avharin@vrngmu.ru](mailto:avharin@vrngmu.ru)  Раб. 8 (473) 210-49-716 (217)  Моб. 8 (951) 569-92-74 |
| **Начальник УИТ**  Донских Александр Игоревич  [a.i.donskih@vrngmu.ru](mailto:a.i.donskih@vrngmu.ru)  Раб.8 (473) 255-46-16  Моб.8 (960) 129-68-81 | **Ведущий инженер ОЦТТО –**  **специалист по защите информации**  Богдан Екатерина Владимировна  [ebogdan@vrngmu.ru](mailto:ebogdan@vrngmu.ru)  Раб. Раб. 8 (473) 210-49-716 (218)  Моб. 8 (904) 212-56-69 |