Приложение № 1

УТВЕЖДЕНА
приказом СП ФГБУЗ ЮОМЦ ФМБА России

от «18» 10 2021 г. № 2734

Политика информационной безопасности
СП ФГБУЗ ЮОМЦ ФМБА России

1. Общие положения

1.1. Настоящая Политика информационной безопасности (далее по тексту Политика ИБ) содержит рекомендации и правила по информационной безопасности для Стоматологической полклиники Федерального государственного бюджетного учреждения здравоохранения «Южного окружного медицинского центра Федерального медико-биологического агентства» (Далее -СП).

1.2. Политика ИБ содержит рекомендации и правила, направленные на снижение рисков нанесения финансового ущерба СП ФГБУЗ ЮОМЦ ФМБА России, ее репутации, умышленного или по неосторожности (халатности) разглашения информации, несанкционированное распространение которой запрещено законами Российской Федерации (далее - РФ) и внутренними нормативными документами СП (далее - защищаемая информация).

1.3. Работники СП несут ответственность за правонарушения с использованием систем автоматизированной обработки информации в соответствии с положениями статей 272, 273, 274 Уголовного кодекса РФ.

2. Защита информации

2.1. Компьютеры пользователей, подключенные к сети Интернет, являются основным вектором атак злоумышленников на СП.

2.2. Для защиты информации СП использует стандартные в своей отрасли технические и организационные меры. Все корпоративные данные хранятся на контролируемых серверах с ограниченным доступом. Передача защищаемой информации организациям, поставщикам оформляется надлежащими соглашениями о конфиденциальности или соглашениями о защищённом документообороте.

2.3. Передача защищаемой информации через незащищенное соединение в сети Интернет осуществляется только при условии обеспечения защиты указанной информации от раскрытия и модификации.

2.4. Работники СП принимают все доступные им меры для обеспечения гарантии безопасности и конфиденциальности защищаемой информации, за которую они несут ответственность, и которая им стала известна.

2.5. В СП доступ к корпоративным ресурсам разрешён только для работников, прошедших установленную процедуру согласования доступа. Права предоставляются в соответствии со служебной необходимостью, определяемой руководством. Все

полномочия по доступу являются персональными, указанными явно и проверенными ответственным лицом СП перед предоставлением доступа.

2.6. По запросу на доступ к корпоративным ресурсам предоставляются полномочия минимально необходимые для реализации данного запроса. Принцип наименьших привилегий требует, чтобы в информационной системе, приложении или корпоративной сети пользователь имел возможность доступа только к той информации и ресурсам, которые необходимы для выполнения его служебных обязанностей.

3. Защита от вредоносного ПО

3.1. В СП используются средства для защиты от вредоносного ПО (антивирусы). Однако, только антивирусной защиты в случае использования сети Интернет, недостаточно, так как существуют угрозы, которые могут не обнаруживаться антивирусами. Поэтому очень важно помнить о том, что нельзя открывать вложения в электронных письмах или переходить по ссылкам, полученным от неизвестных отправителей, а также загружать файлы с подозрительных сайтов в сети Интернет.

3.2. С целью защиты от киберугроз, в СП применяются механизмы блокирования нежелательных веб-ресурсов.

4. Поведение в сети Интернет

4.1. Не посещайте сомнительные ресурсы в сети Интернет.

4.2. Не размещайте в сети Интернет информацию, которая может навредить интересам СП, где вы работаете, и(или) вам лично.

4.3. На всех платформах в сети Интернет, где у вас есть аккаунты и где позволяет соответствующий сервис, необходимо включать двухфакторную аутентификацию. Эта мера может помочь, если пароль для входа в аккаунт стал известен третьим лицам.

4.4. Не сообщайте в социальных сетях персональный адрес корпоративной электронной почты в неслужебных целях.

4.5. Не подписывайтесь на рассылку информации неслужебного характера на персональный адрес корпоративной электронной почты.

4.6. Не обсуждайте в социальных сетях подробности вашей работы.

5. Пароли

5.1. Для получения доступа к корпоративной сети СП, к закрытым сервисам и программам требуется ввести имя пользователя и пароль. Работник СП самостоятельно отвечает за сохранение в тайне сведений об его имени как пользователя и пароле.

5.2. Пароли пользователя СП должны удовлетворять следующим условиям:

– длина пароля должна составлять не менее восьми символов;

– в пароле должны присутствовать большие и маленькие буквы латинского алфавита, цифры и спецсимволы;

– пароли от разных систем и сервисов не должны повторяться.

5.3. При подозрении на компрометацию своего пароля работник должен незамедлительно сообщить об этом своему руководителю и инженер по защите информации.

6. Обновление программ

6.1. На рабочем компьютере настроено автоматическое обновление всех программ, включая операционную систему компьютера. Если обновления устанавливаются вручную, дистрибутивы скачиваются только с сайтов производителей.

6.2. Программное обеспечение СП необходимо дополнять инструментами, которые будут отслеживать наличие уязвимостей и отсутствие обновлений в программах и операционных системах, поскольку злоумышленники нередко используют уязвимости, чтобы проникнуть на рабочие станции пользователей, а затем в корпоративную сеть СП.

7. Мобильные устройства*

7.1. Использование личных мобильных устройств в рабочих целях, несёт дополнительные риски, связанные с защитой информации.

7.2. Не оставляйте мобильные устройства без присмотра в общественном месте и не передавайте их никому в пользование.

7.3. Не создавайте на мобильных устройствах (корпоративных и личных) дополнительные (нелегитимные) сети (например: Wi-Fi) с целью передачи/получения информации.

**Под мобильными устройствами в данном контексте подразумеваются любые переносимые устройства: ноутбуки, смартфоны, планшеты и прочее.*

8. Шифрование

8.1. Если на ваших устройствах хранится защищаемая информация, их следует шифровать, чтобы никто не смог ими воспользоваться в случае потери или кражи устройства.

8.2. Для защиты электронных сообщений от доступа к ним посторонних лиц при передаче по незащищенным каналам связи применяется шифрование.

9. Электронная почта

9.1. Не открывайте электронные сообщения от незнакомых отравителей.

9.2. Корпоративная электронная почта используется только для деловой переписки между работниками и контрагентами.

10. Работа с носителями информации

10.1. Каждый работник СП несет персональную ответственность за использование носителей информации и обязан обеспечить их безопасное хранение. Категорически запрещается снимать несанкционированные копии с носителей с защищаемой информацией, знакомить с содержанием указанной информации лиц, не допущенных к работе с этой информацией, выносить оборудование, носители информации (в том числе бумажные) и программы за пределы СП без письменного разрешения руководства (в том числе для технического обслуживания, ремонта или утилизации).

10.2. Всегда принудительно проверяйте с помощью средств антивирусной защиты съёмные носители информации после использования их вне зданий СП.

10.3. Используйте только разрешенные к применению носители информации.

11. Защита данных на рабочих станциях пользователей и серверах

11.1. Объекты информационной инфраструктуры (в том числе, рабочие станции), прикладное программное обеспечение, технологии обработки защищаемой информации являются собственностью СП и могут быть использованы только в служебных целях.

11.2. Покидая рабочее место, не забывайте блокировать компьютер нажатием комбинации клавиш CTRL-ALT-DEL.

11.3. Не оставляйте гостей на территории СП без сопровождения. Не забывайте закрывать двери в помещение, в которую посторонним вход воспрещен.

11.4. Измельчайте все бумажные документы, содержащие защищаемую информацию. Не забывайте распечатанные документы в принтере.