ГБУК «САХАЛИНСКАЯ ОБЛАСТНАЯ УНИВЕРСАЛЬНАЯ НАУЧНАЯ БИБЛИОТЕКА»

П Р И К А З

«11» марта 2022 г. **№ 116-п**

г. Южно-Сахалинск

О повышении защищенности объектов информационной инфраструктуры ГБУК СахОУНБ

В соответствии с поступившими указаниями ФСТЭК России и необходимостью организационно-технических мер по повышению защищенности информационной инфраструктуры и распоряжением министерства культуры и архивного дела Сахалинской области № 91-р от 02.03.2022 и письма № 3.31-608/22 от05.03.2022 министерства цифрового и технологического развития Сахалинской обла

ПРИКАЗЫВАЮ:

1. Орлову И. Н., заведующему ОВИТ и Соловьевой С. В. в целях проведения информирования о необходимости соблюдения требований по безопасности и принятия мер по блокированию угроз при предоставлении услуг поставщиками продуктов и услуг в сфере информационных технологий, подрядных организаций в сфере информационных технологий, иных юридических и физических лиц, имеющих доступ к объектам информационной инфраструктуры, использовать типовую форму информационного сообщения (Приложение 1).
2. Всем сотрудникам библиотеки для проведения видеоконференций использовать систему TrueConf.
3. Орлову И. Н., заведующему ОВИТ провести организационные и технические работы по исключению возможности применения неучтенных съемных машинных носителей информации и мобильных устройств в срок до 04.04.2022 г.
4. Контроль за исполнение настоящего приказа возложить на заместителя директора по основной деятельности и ИТ Туркину О. Д.

Директор ГБУК СахОУНБ В. А. Малышева

Приложение 1

Уважаемые коллеги!

В связи со сложной геополитической ситуацией, в целях повышения защищенности информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления (далее - объекты ИИ) ГБУК «Сахалинская областная универсальная научная библиотека» уведомляет о необходимости соблюдения требований по безопасности и принятии мер по блокированию угроз при предоставлении услуг поставщиками продуктов и услуг в сфере информационных технологий, подрядных организаций в сфере информационных технологий, иных юридических и физических лиц, имеющих доступ к объектам ИИ, в т.ч. на рабочих местах и ином оборудовании, которые используются для предоставления доступа к объектам ИИ.

К указанным мерам в том числе относятся:

l) организация межсетевого экранирования рабочих мест и оборудования участвующего в предоставлении доступа к объектам ИИ;

2) анализ уязвимостей на рабочих местах и оборудовании участвующих в предоставлении доступа к объектам ИИ, в том числе уязвимостей конфигурации программного обеспечения узлов, включая прикладное и системное программное обеспечение, прошивки оборудования и принятие мер по устранению найденных критических уязвимостей;

3) аудит прав доступа и смена аутентификаторов учетных записей пользователей программного обеспечения, установленного на соответствующих узлах сети, участвующих в предоставлении доступа к объектам ИИ. Соблюдения требований, предъявляемые к парольной защите, на всех объектам ИИ (исключение стандартных, «слабых» и легко угадываемых паролей (например, admin, 1234, passw0rd, и т.п.).

4) ограничение возможности удаленного управления прикладным и системным программным обеспечением, телекоммуникационным оборудованием, участвующим при предоставлении доступа к объектам ИИ органов власти через сеть Интернет;

5) исключение применения иностранных систем видеоконференции, в том числе Zoom, Skype, а также систем удаленного доступа (RAdmin, TeamViewer, Anydesk) при проведении работ на объектах ИИ органов власти;

6) своевременное проведение обновлений баз данных средств антивирусной защиты и разрешающих правил средств обнаружения

вторжений (при их наличии) на рабочих местах и оборудование участвующем в предоставлении доступа к объектам ИИ.