МИНИСТЕРСТВО ОБРАЗОВАНИЯ НОВОСИБИРСКОЙ ОБЛАСТИ

ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ПРОФЕССИОНАЛЬНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ НОВОСИБИРСКОЙ ОБЛАСТИ «БЕРДСКИЙ ПОЛИТЕХНИЧЕСКИЙ КОЛЛЕДЖ» (ГБПОУ НСО «БПК»)

П Р И К А З

14.03.202 № 41-д

г. Бердск

О мерах по повышению защищенности информационных инфраструктур

На основании письма Министерства образования Новосибирской области «О мерах по повышению защищенности информационных инфраструктур» № 2396-09/25 от 10.03.2022, **приказываю:**

1. Заведующему информационных технологий Сластён А.А.

1.1 усилить требования к парольной политике администраторов и пользователей сайтов органов государственной власти, исключив при этом использование паролей, заданных по умолчанию, отключить сервисные и неиспользуемые учетные записи.

1.2 Провести инвентаризацию служб и веб-сервисов, используемых для функционирования официальных сайтов органов государственной власти и размещенных на периметре информационной инфраструктуры (далее – службы и веб-сервисы).

1.3 Обновить службы и веб-сервисы, функционирующие на периметре информационной инфраструктуры.

1.4 Отключить неиспользуемые службы и веб-сервисы.

1.5 Обеспечить поддержку сайтами органов государственной власти соединения с применением защищенных протоколов сетевого взаимодействия (HTTPS, SSH и других протоколов). Использовать только актуальные версии таких протоколов. Также запретить использовать ссылки на сайты с заголовками HTTP даже в теле страниц веб-приложения, поскольку при переходе по такой ссылке есть риск перехвата файлов cookie пользователей.

1.6 Обеспечить фильтрацию сетевого трафика с целью исключения возможности подключения внешних пользователей к TCP-интерфейсам систем управления базами данных и интерфейсам удаленного управления компонентами сайтов. Оставить доступными для подключения внешних пользователей только веб-интерфейсы 443/TCP (HTTPS) и 80/TCP (с принудительным перенаправлением на порт 443/TCP с HTTPS); исключить возможность применения на сайтах органов власти сервисов подсчета сбора данных о посетителях, сервисов предоставления информации о месторасположении и иных сервисов, разработанных иностранными организациями (например, сервисов onthe.ioReCAPTCHA, YouTube, Google Analytics, Google Maps, Google Translate, Google Analytics);

1.7 Исключить возможность использования встроенных видео- и аудио-файлов, интерфейсов взаимодействия API, «виджетов» и других ресурсов,

загружаемых со сторонних сайтов, заменив их при необходимости гиперссылкой на такие ресурсы.

1.8 В целях повышения устойчивости сайтов органов власти к распределенным атакам, направленным на отказ в обслуживании (DDoS-атакам) необходимо принять следующие первоочередные меры защиты информации.

1.9 Обеспечить настройку правил средств межсетевого экранирования на блокировку не разрешенного входящего трафика;

1.10 Обеспечить фильтрацию трафика прикладного уровня с применением средств межсетевого экранирования уровня приложения (web application firewall (WAF)), установленных в режим противодействия атакам.

1.11 Активировать функции защиты от DDoS-атак на средствах межсетевого экранирования и других средствах защиты информации.

1.12 Ограничить количество подключений с каждого IP-адреса (например, установить на веб-сервере параметр raid-limit).

1.13 Блокировать входящий трафик, поступающий с IP-адресов, страной происхождения которых являются США, страны Европейского союза или иной страной, являющейся источником компьютерных атак.

1.14 Блокировать трафик, поступающий из «теневого Интернета» (сети Tor) (список узлов, которые необходимо заблокировать содержатся по адресу https://www.dan.me.uk/tornodes).

1.15 Обеспечить фильтрацию трафика прикладного уровня с применением средств межсетевого экранирования уровня приложения (web application firewall (WAF)), установленных в режим противодействия атакам.

1.16 Проинформировать администраторов и пользователей информационных систем о недопущении распространения информации о функционировании информационной системы, передаче сторонним лицам своей аутентификационной информации.

1.17 Проинформировать администраторов и пользователей информационных систем об ответственности за нарушение требований в области информационной безопасности.

1.18 Усилить контроль над действиями в информационной системе администраторов и пользователей.

1.19 Провести внеплановую смену паролей администраторов и пользователей, используемых для доступа в информационные системы.

1.20 Исключить (при возможности) удаленный доступ посредством сети «Интернет» к информационным системам для администраторов и пользователей;

1.21 обеспечить (при возможности) двухфакторную аутентификацию администраторов информационных систем.

1.22 настроить правила доступа для всех категорий пользователей веб-серверов к файлам и каталогам веб-сервера в соответствии с установленными правилами разграничения доступа (например, для пользователей, от имени которых запускается веб-сервер, для пользователей ftp-серверов и пользователей других служб).

1.23 Установить минимально необходимые для работы права доступа к файлам и директориям веб-серверов пользователям и администраторам.

1.24 Ограничить доступ к каталогам систем контроля версий и их содержимому (таким как: git, .svn и другие каталоги).

1.25 Настроить запрет выдачи листинга каталогов при отсутствии в них индексируемых файлов (если иное не предусмотрено функциональными возможностями веб-сервера).

1.26 Настроить с использованием файла с именем robots.txt разрешенные и запрещенные для индексации каталоги, и файлы.

1.27 Ограничить хранение в директориях веб-сервера резервных копий и прочих файлов, наличие которых не требуется для функционирования веб-приложения.

1.28 Ограничить использование на веб-страницах серверов информационных ресурсов (видеофайлов, электронных документов, изображений и других файлов), размещенных на сторонних серверах. Обеспечить резервирование информации, обрабатываемой в информационной системе, и проверить наличие актуальных резервных копий.

1.29 Обеспечить хранение резервных копий в изолированном от сети «Интернет» сегменте информационной системы.

1.30 Ограничить доступ пользователей информационной системы к резервным копиям данных.

1.31 Ограничить (при возможности) сетевое взаимодействие между сегментами информационных систем по принципу «запрещено всё, что явно неразрешено» (например, с помощью технологии VLAN и списков контроля доступа сетевого оборудования).

1.32 Активировать функции анализа и блокировки входящего сетевого трафика средств межсетевого экранирования, установленных на рабочих местах пользователей (при их наличии).

1.33 Ограничить доступ пользователей информационной системы и доступ внешних пользователей из сети «Интернет» к системам централизованного управления инфраструктурой информационных систем (при их наличии) (например, к таким системам относятся Active Directory, SCCM, Zabbix и другие системы).

1.34 Провести анализ защищенности периметра информационной системы и веб-серверов в части выявления и устранения критических уязвимостей, ошибок конфигурации, а также удаления паролей, используемых по умолчанию.

1.35 Запретить пользователям подключать к информационным системам неучтенные машинные носители информации, мобильные устройства и открывать любые ссылки из почтовых сообщений, скачивать файлы из сети «Интернет», а также использовать мобильные устройства для подключения к сети «Интернет».

1.36 Ограничить (при возможности) администраторам информационных систем права по сетевому подключению к автоматизированным рабочим местам пользователей.

1.37 Ограничить средствами прокси-сервера список внешних информационных ресурсов, к которым пользователи информационной системы.

1.38 Организовать доступ к удаленным сегментам информационных систем (при их наличии) с применением виртуальных частных сетей (VPN).

1.39 Ограничить использование беспроводных сетей (wi-fi).

1.40 Обеспечить применение средств антивирусной защиты и антиспама, а также своевременное обновление их баз данных

1.41 Настроить в средствах антивирусной защиты, антиспама (при

наличии) проверку всех поступающих на почту вложений.

2. Проинформировать сотрудников-пользователей информационной системы о необходимости безопасной работы с электронной почтой, а именно.

2.1 Внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом.

2.2 Не открывать письма от неизвестных адресатов.

2.3 Проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы.

2.4 Не переходить по ссылкам, которые содержаться в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.).

2.5 Не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов.

2.6 Проверять ссылки, даже если письмо получено от другого пользователя информационной системы.

2.7 Не открывать вложения, особенно если в них содержаться документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, CHM, VHD.

2.8 Внимательно относиться к письмам на иностранном языке, с большим количеством получателей и орфографическими ошибками.

2.9 В случае появления сомнений - направлять полученное письмо как вложение администратору информационной системы.

2.10 Заблокировать (при возможности) получение пользователя информационной системы в электронных письмах вложений с расширениями AOE, ADP, APK, APPX, APPXBUNDLE, BAT, CAB, CHM, CMD, COM, CPL, DLL, DMG, EX, EX_, EXE, HTA, INS, ISP, ISO, JAR, JS, JSE, LIB, LNK, MDE, MSC, MSI, MSIX, MSIXBUNDLE, MSP, MST, NSH, PIF, PS1, SCR, SCT, SHB, SYS, VB, VBE, VBS, VHD, VXD, WSC, WSF, WSH.

2.11 Заблокировать доставку писем от доменов-отправителей, страной происхождения которых являются США и страны Европейского союза.

3. Ответственность за размещение приказа возложить на заведующего отделом информационных технологий Сластён А.А

4. Контроль за исполнением приказа возложить на заместителя директора по безопасности Устинова В.Б.

Директор  Р.К. Устинова

А.А. Сластён
8(383)-41-42482

_____Сластён А.А.

_____Устинов В.Б.