Инструкция по безопасной работе на компьютере в информационных сетях.

1. Использование и установка на всех автоматизированных рабочих местах средств антивирусной защиты, включенных в Реестр российского программного обеспечения.
2. Запрет на подключение к компьютеру неучтенных устройств и съемных носителей.
3. Хранение логинов, паролей и электронных подписей в недоступном месте.
4. Регулярная смена паролей и обновление программного обеспечения.
5. Обеспечение регулярного резервного копирования информации.
6. Обязательное выключение компьютера в нерабочее время.
7. Запрет на доступ к ресурсам через бесплатные беспроводные сети (free wi-fi zone).

Памятка по работе с электронной почтой и фишинговыми письмами.

Официальная почта должна быть создана с использованием доменных имен (ru.; su.; рф.) и сетевых адресов, находящихся в российской национальной доменной зоне.

С целью предотвращения реализации угроз безопасности информации, связанных с фишингом, необходимо принять следующие меры защиты информации:

1. внимательно проверять адрес отправителя, даже в случае совпадения имени с уже известным контактом;
2. не открывать письма от неизвестных адресатов;
3. проверять письма, в которых содержатся призывы к действиям (например, «открой», «прочитай», «ознакомься»), а также с темами про финансы, банки, геополитическую обстановку или угрозы;
4. не переходить по ссылкам, которые содержатся в электронных письмах, особенно если они длинные или наоборот, используют сервисы сокращения ссылок (bit.ly, tinyurl.com и т.д.)
5. не нажимать на ссылки из письма, если они заменены на слова, не наводить на них мышкой и просматривать полный адрес сайтов;
6. проверять ссылки, даже если письмо получено от другого пользователя информационной системы;
7. не открывать вложения, особенно если в них содержатся документы с макросами, архивы с паролями, а также файлы с расширениями RTF, LNK, C HM, VHD;
8. внимательно относиться к письмам на иностранном языке, с большим количеством получателей;
9. в случае обнаружения фактов массовой рассылки незамедлительно сообщить в отдел информатизации и связи администрации Калининского района (denisov@tukalin.gov.spb.ru, komarova@tukalin.gov.spb.ru).

Все подозрительные электронные письма отправлять на адрес электронной почты: antivirus@gov.spb.ru.

Дополнительные рекомендации по работе с электронной почтой

1. Настроить в средствах антивирусной защиты, антиспама (при наличии) проверку всех поступающих на почту вложений.

2. Заблокировать (при возможности) получение пользователями информационной системы в электронных письмах вложений с расширениями ADE, 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.

3. Заблокировать доставку писем от доменов-отправителей стран, поддержавших санкции Украины, США и стран Европейского союза.

Памятка по работе с официальными страницами в социальной сети «Вконтакте».

1. Обеспечить регистрацию (актуализацию) официальных страниц в социальной сети «ВКонтакте» путем подтверждения государственного статуса сообщества через Госуслуги.
2. Осуществление ежедневного мониторинга официальных страниц в социальной сети «ВКонтакте» с целью выявления информации, запрещенной к распространению законодательством Российской Федерации.
3. Обязательная смена паролей и передача прав администратора при увольнении сотрудников (дополнительная инструкция: https://disk.yandex.ru/i/k4SP0flVIGkXiw)..
4. Использование надежных паролей с двухфакторной аутентификацией в социальной сети «ВКонтакте» (https://connect.vk.com/account/#/otp-settings).
5. Использование на официальных страницах учреждений в социальной сети «ВКонтакте» фильтров нецензурных выражений, враждебных высказываний и фильтра по ключевым словам (дополнительная инструкция).
6. Указать возрастные ограничения до 16 лет (дополнительная инструкция).
7. О всех фактах выявленных нарушений (адрес сайта в сети интернет, адрес страницы с выявленным нарушением, дата обнаружения нарушения) и принятых мерах (перечень действий организации по устранению, дата устранения), прошу сообщать в администрацию Калининского района, Комитет по информатизации и связи и Комитет по образованию не позднее дня обнаружения нарушения по следующим адресам электронных почт:

denisov@tukalin.gov.spb.ru
komarova@tukalin.gov.spb.ru
soc-spb@iac.spb.ru;
o.novoslugina@iac.spb.ru;
trifonov@iac.spb.ru;
tokareva@kis.gov.spb.ru;
puchkov@kobr.gov.spb.ru;
info.cokoit@obr.gov.spb.ru;
it-info@kobr.gov.spb.ru

Памятка по работе с официальными сайтами в сети Интернет.

1. Обеспечить регистрацию (актуализацию) официальных сайтов путем их включения в «Единую систему информационных ресурсов официальных сайтов исполнительных органов государственной власти Санкт-Петербурга и государственных учреждений Санкт-Петербурга» (АСИ «ЕСИР»).
2. Осуществление ежедневного мониторинга официальных сайтов с целью выявления информации, запрещенной к распространению законодательством Российской Федерации.
3. Обязательная смена паролей при увольнении сотрудников и смене системных администраторов.
4. Отключение комментариев на официальных сайтах при условии возможности их написания другими пользователями.
5. В случае обнаружения в поисковых интернет системах сайтов, позволяющих идентифицироваться как сайт государственного учреждения, а также старые, неиспользуемые домены учреждений и невозможности их самостоятельной блокировки, сообщить адреса указанных сайтов в отдел информатизации и связи администрации Калининского района (denisov@tukalin.gov.spb.ru, komarova@tukalin.gov.spb.ru).

О всех фактах выявленных нарушений (адрес сайта в сети интернет, адрес страницы с выявленным нарушением, дата обнаружения нарушения) и принятых мерах (перечень действий организации по устранению, дата устранения), прошу сообщать в администрацию Калининского района, Комитет по информатизации и связи и Комитет по образованию не позднее дня обнаружения нарушения по следующим адресам электронных почт:

denisov@tukalin.gov.spb.ru
komarova@tukalin.gov.spb.ru
soc-spb@iac.spb.ru;
o.novoslugina@iac.spb.ru;
trifonov@iac.spb.ru;
tokareva@kis.gov.spb.ru;
puchkov@kobr.gov.spb.ru;
info.cokoit@obr.gov.spb.ru;
it-info@kobr.gov.spb.ru