Москва, 14.01.2022

Проблемы информационной безопасности: новые угрозы для офисных печатающих устройств и защита от них

Москва, 14 января 2021 г. — Информационное Агентство «Бизнес-Информ» и Ассоциация Производителей и Поставщиков Качественных Расходных Материалов представили новые результаты исследований уязвимостей офисных печатающих устройств и рекомендации по их устранению

Информационное Агентство «Бизнес-Информ» и Ассоциация Производителей и Поставщиков Качественных Расходных Материалов (АППКРМ) 14 января текущего года провели конференцию **«Проблемы информационной безопасности: новые угрозы для офисных печатающих устройств и защита от них».** На конференции были продемонстрированы результаты новых исследований уязвимостей офисных печатающих устройств, обнаруженные в российских и зарубежных организациях в 2021 году, а также рекомендации по их устранению. Особое внимание на конференции было уделено современным политикам информационной защиты корпоративных сетей предприятий, прежде всего - политике "нулевого доверия", а также вопросам, связанным с практикой эксплуатации систем документооборота (ИТ-аутсорсинг, MPS, использование восстановленных картриджей и картриджей-новоделов). В конференции приняли участие представители 162 российских предприятий и организаций, а также ведущие российские и зарубежные эксперты в области информационной безопасности.

На конференции были заслушаны 3 доклада:

- **«Принтеры, копиры, МФУ и картриджи - источники уязвимостей. Аудит печатающих устройств в российских организациях в 2021 году: результаты, выводы и рекомендации»** (докладчик — Малинский С.В., Российский Университет Транспорта)

Тезисы доклада: Офисная печать и ее организация: правовые, административные и программно-технические аспекты. Микропрограммное, системное и прикладное программное обеспечение: уязвимости явные и скрытые, методы пассивной и активной защиты. Ведущие бренды-производители печатающих устройств и их политика в области обеспечения информационной безопасности. HP и фирменное микропрограммное обеспечение FutureSmart: уязвимости CVE-2021-39237 (CVSS score: 7.1) и CVE-2021-39238 (CVSS score: 9.3) и как от них защищаться. Прошел месяц - и новые сюрпризы CVE-2021-44228, CVE-2021-45046, CVE-2021-4104, CVE-2021-45105, CVE-2021-44832 и их последствия. KonicaMinolta и обнаруженные ею уязвимости CVE-2021-20868, CVE-2021-20869, CVE-2021-20870, CVE-2021-20871, CVE-2021-20872: как от них защищаться и надо ли это делать? Печатающие устройства Brother, Canon, Lexmark, Ricoh, Xerox - вакцинация не гарантирует защиты от вирусов. Актуально: так нужно ли разрабатывать новые вакцины и вакцинироваться? Пассивные и активные методы защиты и законодательные ограничения на их применение. Аудит печатающих устройств в российских организациях в 2021 году: основные результаты и выводы. Скупой платит дважды, тупой - трижды, лох - всю жизнь. Для защиты здоровья необходима, как минимум, элементарная гигиена или почему не надо сразу включать и начинать печатать на новом МФУ.

- **«Модель нулевого доверия: рекомендации по внедрению и возможные проблемы»** (докладчик – Малинский С.В., Российский Университет Транспорта)

Тезисы доклада: Рост преступности в период пандемии. ZeroTrust («нулевое доверие») – это модель безопасности, предполагающая полное отсутствие доверия к какому-либо пользователю, устройству, приложению. Основные компоненты архитектуры нулевого доверия согласно «NIST Special Publication 800-207: ZeroTrust Architecture». Семь принципов нулевого доверия и особенности их реализации в современных системах автоматизированного документооборота. Минимальные контрольные требования нулевого доверия. Рекомендации по внедрению нулевого доверия. Проблемы, связанные с внедрением нулевого доверия на практике. Требования нулевого доверия к операционным системам и устройствам ввода/вывода и их функционалу. Обновление ПО как новый источник уязвимостей. Оригинальные и неоригинальные картриджи несут новые угрозы. Превентивные меры защиты. Необходимость непрерывного мониторинга сети. Если кража информации неизбежна, на помощь приходят криптография и стеганография. Уточнения существующих политик информационной безопасности неизбежны. Тенденции развития российского рынка офисной печати в новых условиях.

Этот доклад получил Диплом "За лучший научный доклад" на Всероссийской научно-теоретической конференции "Теория и практика обеспечения информационной безопасности ТиПОИБ-2021" в секции "Криптографические алгоритмы и сетевая безопасность"

- **«Принтеры, МФУ и картриджи – источники уязвимостей. Рекомендации по приобретению, эксплуатации и утилизации в 2022 году. Ответственность поставщиков и пользователей в соответствии с законодательством РФ»** (докладчики — Семенов А.И., Юридическое Агентство «Бизнес-Информ», Савинова А.А., Информационное Агентство «Бизнес-Информ»)

Тезисы доклада: Офисная печать и ее организация: программно-технические аспекты. Дыры в системном и прикладном программном обеспечении. Патчи и их роль для хакеров и специалистов по ИБ. Принтеры и МФУ как источники уязвимостей. Решения производителей печатающих устройств и можно ли им доверять? Сертификаты по ИБ печатающих устройств, и какое отношение они имеют к российскому рынку. Встроенное ПО и его обновление. Какие цели преследуют производители? Удаленные рабочие места приносят новые проблемы. Картриджи (оригинальные, восстановленные и новоделы) и чипы – еще одни группа вопросов по ИБ. Что делает чип: заявления изготовителей и мнение исследователей по ИБ. Шпионская техника и что о ней написано в УК РФ и КоАП РФ. Обзор судебной практики, начиная с 13 августа 2019 года. Ответственность поставщиков и ответственность пользователей. Проблемы утилизации печатающих устройств и расходных материалов для специалистов по ИБ: обзор ошибочных решений и рекомендации по практической деятельности в 2022 году.

Участники конференции обсудили с докладчиками представленную информацию, результаты исследований уязвимостей офисных печатающих устройств, обнаруженных в российских и зарубежных организациях в 2021 году, а также рекомендации по их устранению. Особое внимание участники конференции уделили современным политикам информационной защиты корпоративных сетей предприятий, а также вопросам, связанным с практикой эксплуатации систем документооборота (ИТ-аутсорсинг, MPS, использование восстановленных картриджей и картриджей-новоделов). Участники конференции поздравили одного из докладчиков - Малинского С.В. - с награждением его Дипломом "За лучший научный доклад" на Всероссийской научно-теоретической конференции "Теория и практика обеспечения информационной безопасности ТиПОИБ-2021" в секции "Криптографические алгоритмы и сетевая безопасность".

Приятным подарком для всех участников конференции стали новые выпуски журнала BUSINESS-INFORM Review (выпуск №3, 2021) и его приложения «Экспертиза и Качество» (декабрь, 2021).

АППКРМ info@aqcmsrus.ru, https://aqcmsrus.ru/

БИЗНЕС-ИНФОРМ bizinform@list.ru, http://sforp.ru/