3. *Сарна А.Я.* Технологии воздействия на аудиторию в современном медиапространстве // Вестник Санкт-Петербургского университета. Социология. – 2020. – Т. 13. № 2. – С. 218-235.

4. *Волгина О.А., Нечаева П.А.* Численное моделирование процессов распространения активности в социальных сетях на основе моделирования гетерогенных взаимодействий MIMO-агентов / Материалы Межвузовской научно-технической конференции студентов, аспирантов и молодых специалистов имени Е.В. Арменского. – М.: МИЭМ НИУ ВШЭ, 2022. – С. 10-12.

5. *Волгина О.А., Нечаева П.А.* Влияние типов агентов на распределение мнений в социальных сетях / Труды 19-ой Всероссийской школы-конференции молодых ученых «Управление большими системами» (УБС'2023, Воронеж) (в печати).

6. *Дашкова А.Ю.* Манипулятивные методы воздействия на массовое сознание // Вестник Поволжского института управления. – 2010. – № 1. – С. 74-77.

7. *Науменко Т.В.* Психологические методы воздействия на массовую аудиторию // Вопросы психологии. – 2003. – № 6. – С. 112-125.

DOI: 10.25728/iccss.2023.65.61.040

Зорин В.А., Ненашева Ю.А., Галин Р.Р., Мещеряков Р.В.

Противодействие фишингу с использованием беспилотных аппаратов на публичные Wi-Fi-сети на массовых мероприятиях

Аннотация: Рассмотрен способ фишинга с использованием беспилотных аппаратов и публичных Wi-Fi-сетей на массовых мероприятиях. Приведены предложения для снижения возможности успешных атак.

Ключевые слова: фишинг, анализ уязвимостей, беспилотные аппараты

Публичные массовые мероприятия проводятся с целью повышения культурного и духовно-нравственного уровня населения, вовлечения в социальные и спортивно-оздоровительные проекты и программы. Злоумышленники ставят цели компрометации и дискредитации организаторов массовых

мероприятий, а также сбора средств для финансирования преступной деятельности.

Традиционно на время подготовки и проведения мероприятия разворачивается сеть Wi-Fi с доступом для организаторов и посетителей. Следует отметить, что среди абонентов сети можно выделить уязвимые группы пользователей, в том числе высокопоставленные гости.

Доступ к Wi-Fi-сетям предоставляется после авторизации. Выделим существующие способы авторизации в Wi-Fi-сетях.

1. Авторизация пользователей публичного Wi-Fi по звонку. По исходящему звонку: пользователь вводит свой номер телефона, звонит на бесплатный номер, звонок отклоняется и предоставляется доступ в интернет. По входящему звонку: Пользователь вводит свой номер телефона и получает входящий звонок со случайного номера из перечня доступных оператору мероприятия. Для доступа требуется ввести четыре последних цифры номера в качестве кода доступа.

2. Авторизация пользователей публичного Wi-Fi по ваучеру. Система авторизации по ваучерам позволяет давать пользователям доступ к Wi-Fi по уникальному логину и паролю. Логин и пароль автоматически генерирует система при создании нового ваучера. В системе хранятся данные о потенциальном пользователе, которому будет выдан ваучер: номер аккредитации, номер паспорта, номер телефона, срок действия пароля. Данный способ Wi-Fi авторизации подходит также и для иностранных граждан, у которых нет возможности зарегистрироваться с помощью SMS или звонка из-за роуминга.

3. Авторизация пользователей публичного Wi-Fi через Госуслуги. Авторизация через данные учетной записи на сайте Госуслуг (www.gosuslugi.ru).

4. Авторизация пользователей публичного Wi-Fi по SMS. Пользователь вводит свой номер телефона, получает sms-сообщение с кодом доступа, вводит код и выходит в интернет. Этот способ привычен для пользователей, поэтому представляет наибольшую угрозу с точки зрения потенциального фишинга.

В настоящей работе рассмотрена модель реализации фишинга при авторизации пользователей публичного Wi-Fi и способы противодействия.

В качестве реализации угрозы рассмотрен следующий вектор атаки.

1. Злоумышленник создает подменную страницу авторизации аналогичной страницы организатора, на которой выведена просьба ввести телефон и поле для ввода пароля.

2. С помощью беспилотного аппарата доставляет нелегальную точку доступа с похожим SSID к месту расположения атакуемой группы высокопоставленных гостей или представителей организаторов. Данный способ, в том числе, позволяет исключить использование канала управления для беспилотного аппарата.

3. С подменной страницы данные перенаправляются на сервера мессенджеров для смены устройства. Такая схема используется злоумышленниками для захвата аккаунтов в Telegram или в запрещенной в России сети.

После захвата устройства злоумышленник получает доступ к контактам жертвы, где при помощи механизмов социальной инженерии пытается получить финансирование.

Кроме того, на экранах устройств жертв, после захвата мессенджеров может выводиться альтернативная страница с запрещенной символикой и/или противозаконными лозунгами.

Предлагаются следующие способы противодействия.

1. Привлечение на массовые мероприятия представителей Радиочастотной службы для отслеживания в эфире паразитных SSID, а также точек доступа, не находящихся в пуле организатора.

2. Мониторинг использования радиочастотного спектра на предмет несогласованных источников радиоизлучения.

3. Размещение информации на билетах, плакатах и иных стендах о невозможности авторизоваться в Wi-Fi-сетях организаторов с помощью пароля из SMS.

4. Скрыть Wi-Fi сети от пользователей и авторизировать только через QR-код на билетах.

5. Информирование посетителей об основах цифровой гигиены и способах фишинга посредством рекламно-информационных экранов и стендов.

6. Ограничение доступа несогласованных радиоэлектронных средств в места проведения массовых мероприятий.

7. Ограничение или введение повсеместного запрета на авторизацию в Wi-Fi-сетях с использованием пароля из SMS.

В результате анализа атаки фишинга при авторизации пользователей публичного Wi-Fi следует учесть, что данный способ может быть использован практически в любых публичных сетях. Предложены комбинированные способы противодействия, включающие ограничительные меры и обучение населения основам информационной безопасности и цифровой гигиены.

DOI: 10.25728/iccss.2023.99.51.041

Фомин Н.А.

Уязвимости кибер-физических систем. Метод управления и оценивания защищенности кибер-физической системы водоснабжения

Аннотация: Рассмотрены особенности уязвимостей кибер-физических систем водоснабжения (КФСВ). Сформулированы определения – угроза безопасности, уязвимость и риск КФС. Описан метод управления и оценивания защищенности КФСВ.

Ключевые слова: кибербезопасность, кибер-физические системы, методы оценки безопасности, уязвимости, управление системами

Метод управления и оценивания защищенности кибер-физические системы водоснабжения (КФСВ) является элементом создаваемой модели безопасности социально-экономической системы цифрового водоканала. Метод M_1 входит в перечень мероприятий и механизмов формирования политики обеспечения кибербезопасности системы управления рассматриваемого объекта. Метод M_1 отличается от существующих выявлением и классификацией потенциальных уязвимостей, угроз и рисков функционирования КФСВ Умного города. На основе проведенного международного анализа проблем управления [1], сформируем требования к входам и выходам проектируемой модели [2]. На входе модели M_1 международные проблемы безопасности управления, стандарты, сведения о ресурсах, лучшие практики управления водными ресурсами. На выходе – классифицированный перечень потенциальных уязвимостей, угроз и рисков КФСВ (рисунок 1).