Сеспедес Гарсия П.Д.
аспирант,
Научный руководитель: **Федухин А.В.**
доктор технических наук,
Институт проблем математических машин и систем
Национальной академии наук Украины

К ВОПРОСУ О БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

По мере того, как все больше предприятий начинают активно адаптироваться к сложившейся ситуации вынудившей перевести трудовые ресурсы на удалённый режим работы, стратегиям кибербезопасности для защиты компьютерных систем и данных уделяется более приоритетное внимание. В 2020 году большинство руководителей меняет свои стратегии по обеспечению безопасности внутренних комп. систем, и к 2021 году предприятиями планируется увеличение бюджета в этой области несмотря на то, что в целом, ожидается снижение доходов от бизнеса [1]. Рассматривая актуальные прогнозы, основные тренды и векторы развития в сфере кибербезопасности 2020–2021 года, можно выделить несколько основных тенденций, которые встречаются во многих отчетах о прогнозировании [2].

Риски в сфере безопасности компьютерных систем и сетей меняются ежедневно, и необходимо чётко сконцентрировать доступные ресурсы на понимание логики их возникновения. Текущие специалисты обращают внимание на оценку и управление уязвимостями на основе рисков, осваивание инструментальных средств мониторинга и их диагностики, а также развитие методик по принятию решений при выявлении инцидентов информационной безопасности.

Наиболее актуальным и незаменимым методом в вопросе преодоления проблем и повышения уровня кибербезопасности является обучение и повышение осведомленности пользователя на тему правил информационной безопасности. Нарушение этих правил необученным пользователем – это лишь вопрос времени. Используя отработанные фишинговые методы, основанные на социальной инженерии, сложные технические решения становятся излишними, ведь получение злоумышленником полезных данных либо доступа к системе упирается исключительно в степень реализованной психологической манипуляции, либо человеческой слабости [3]. На момент 2021 г., безопасность трудовых ресурсов, а именно удалённая работа на дому, оказывает огромное влияние на общий уровень кибербезопасности. Увеличивается количество атак на домашние персональные компьютеры и сети, используя слабозащищенные системы, либо системы чья поддержка разработчиком системы безопасности и вовсе прекращена (пр.: Windows 7) [4]. Слабые места в архитектуре домашнего рабочего ПК и недостаточный уровень осведомленности пользователя о правилах информационной безопасности, на ряду с ослаблением бдительности пользователя по мере расширения работы на дому станут отправными точками для злоумышленников [5].

Развитие автоматизации программ-вымогателей и фишинга, их адаптирование к облачным репозиториям и эволюция методов злонамеренных атак приводят ко взлому конфиденциальных высокочувствительных данных не только на разного сорта предприятиях и организациях, но также и в критически важных инфраструктурах. В качестве примера, используя текущую ситуацию с COVID-19 как подспорье для проведения масштабных фишинговых атак на широкие группы населения, злоумышленники обманом принуждают пострадавших пользователей предоставить личную и/или рабочую информацию, тем самым ставя под угрозу весь рабочий процесс [6].

Множество сбоев и уязвимостей в вопросах общей безопасности компьютерных систем будут происходить из-за неправильной и/или поспешной конфигурации облачных сервисов и спешки к переходу на них. Из-за перехода на удаленную работу, организации поспешно рассматривают варианты использования облачных сервисов и/или хранения рабочих данных в системах облачных хранилищ, что в последствии, даёт злоумышленникам дополнительную, более широкую область деятельности и возможности для заполучения доступа к системам и данным.

Машинное обучение становится все более распространенным на предприятиях методом для принятия автоматизированных решений, исходя из чего у злоумышленников появляется новый вектор, к

которому, с точки зрения кибербезопасности, следует внимательно присмотреться. Помимо использования технологий ИИ для выявления уязвимостей в технологической инфраструктуре организации и/или конкретной системы, злоумышленник, получивший доступ к копии исходных данных системы использующую методы машинного обучения, может произвести манипуляцию моделями и намеренно исказить данные, тем самым образуя неверно обученную систему, что нарушает целостность обработанных и сгенерированных ею данных [7].

Идентификация и многофакторная аутентификация (Multi-factor authentication) будут также в центре внимания у злоумышленников, поскольку пароли начнут уходить на задний план, в пользу, например, биометрической идентификации. По прогнозам, сервисы и организации не использующие многофакторные методы контроля доступа рано или поздно пострадают от взлома [8].

Еще одним примером потенциальной угрозы кибербезопасности, которая по прогнозам станет довольно актуальной в ближайшие несколько лет, является увеличение количества высоко-профильных взломов Интернета Вещей (Internet of Things) и заражение домашних сетей сетевыми червями. Способствовать этому будет созревание технологии 5G, что приведет к увеличению количества устройств Интернета Вещей, что в свою очередь приведет к возникновению и развитию уязвимостей сети, которые станут более существенными с течением времени [2]. Взаимосвязь между устройствами посредством 5G увеличивает вероятность кибератак из-за отсутствия инфраструктуры безопасности и прозрачности между устройствами [7].

Ближайшие годы, безусловно, будут вызовом для специалистов в вопросах безопасности компьютерных систем, не многим приходило в голову предсказать что влияние глобальной пандемии приведет к серьёзным проблемам кибербезопасности. Однако, судя по прогнозам исследовательских отчетов в данной сфере [2], использование ориентированных на трудовые ресурсы стратегий, которые будут защищать ключевые сервисы, каналы связи и методы хранения конфиденциальных данных, которые необходимы конкретно для удалённой работы, являются приоритетными для увеличения шансов на сохранность рабочего процесса на многих его этапах.

Список использованных источников:

1. The Best Cybersecurity Predictions For 2021 Roundup. URL: https://www.forbes.com/sites/louiscolumbus/2020/12/15/the-best-cybersecurity-predictions-for-2021-roundup/?sh=7e49d08c5e8c (дата обращения: 13.11.2021).

2. The Top 21 Security Predictions for 2021. URL: https://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-21-security-predictions-for-2021.html (дата обращения: 13.11.2021).

3. Ключевые тренды рынка кибербезопасности и защиты информации 2020–2021 в противовес прогнозу 2019–2020 / Хабр. URL: https://habr.com/ru/company/softline/blog/500758/ (дата обращения: 13.11.2021).

4. Windows 7 support ended on January 14, 2020. URL: https://support.microsoft.com/en-us/windows/windows-7-support-ended-on-january-14-2020-b75d4580-2cc7-895a-2c9c-1466d9a53962 (дата обращения: 13.11.2021).

5. Turning the Tide: Trend Micro Security Predictions for 2021 – Security Predictions. URL: https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2021 (дата обращения: 13.11.2021).

6. Seven 2021 Security Predictions and Trends to Watch | Proofpoint US. URL: https://www.proofpoint.com/us/blog/security-briefs/seven-2021-security-predictions-and-trends-watch (дата обращения: 13.11.2021).

7. 10 Cyber Security Trends to Look for in 2021. URL: https://onlinedegrees.und.edu/blog/cyber-security-trends/ (дата обращения: 13.11.2021).

8. 2021 Cybersecurity Predictions | WatchGuard Technologies. URL: https://www.watchguard.com/wgrd-resource-center/cyber-security-predictions-2021 (дата обращения: 13.11.2021).