МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное
учреждение высшего образования
Дальневосточный федеральный университет

ШКОЛА ЕСТЕСТВЕННЫХ НАУК

Кафедра информационной безопасности

О Т Ч Е Т

о прохождении учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики

Выполнил студент
гр. С8118-10.05.01-1спец
_____ Масленников Н.С.
(подпись)

Отчет защищен с оценкой

_____

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

« 31 » июля 2021 г.

Руководитель практики
Старший преподаватель кафедры
информационной безопасности ШЕН

_____ С.С. Зотов
(подпись) (И.О. Фамилия)

Регистрационный № _____
« 31 » июля 2021 г.

_____ Е.В. Третьяк
(подпись) (И.О. Фамилия)

Практика пройдена в срок
с « 19 » июля 2021 г.
по « 31 » июля 2021 г.
на предприятии
Кафедра информационной безопасности ШЕН ДВФУ

г. Владивосток
2021

Содержание

Задание на практику

- Проведение исследования в области информационной безопасности при удалённой работе.
- Написание отчета по практике о проделанной работе.
- Написание тезисов по изучаемой теме.
- Подготовка презентации по проведённому исследованию.

Введение

Учебная (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практика проходила на кафедре информационной безопасности ШЕН ДВФУ в период с 19 июля 2021 года по 31 июля 2021 года.

Целью прохождения практики является приобретение практических и теоретических навыков по специальности, а также навыков оформления проведенного исследования в отчетной форме.

Задачи практики:

1. Ознакомиться с понятием информационной безопасности при удалённой работе.
2. Теоретически ознакомиться с новыми рисками и угрозами безопасности, появившимися во время пандемии.
3. На основе полученных знаний написать отчет по практике о проделанной работе.

Новые угрозы и риски безопасности и конфиденциальности при удалённой работе во время пандемии.

Аннотация:

Мы рассматриваем риски, которые возникли в связи: с увеличением числа импровизированных офисов на дому, степенью отвлекающих факторов, сопровождающих удаленную работу, резким переходом к удаленной работе, резким внедрением различных форм новых технологий/приложений для взаимодействия (например, для работы в Интернете) для взаимодействия (например, Zoom, Microsoft Teams…).

Особый интерес представляет то, как изменились проблемы и решения в области кибербезопасности после COVID-19. Это включает в себя рост числа атак, направленных на удаленных сотрудников и проблемы, с которыми сталкиваются компании при обеспечении безопасности удаленных сотрудников (некоторые из них которые связаны с трудностями использования человеком новых технологий).

Удаленная работа с начала пандемии.

Удаленная работа стала нормой для многих в связи с пандемией. Удалённая работа конечно же, не нова и существует уже долгое время, но усугубила многие из существующих проблем, связанных с этим видом работы.

Это привело к совершенно новому рабочему опыту для миллионов людей, которые никогда раньше не работали удаленно.

Кроме того, у работодателей и работников было мало времени, чтобы подготовиться к массовой потребности в удаленной работе . Это означало, что технологические средства (например, ноутбуки, домашние офисы или программное обеспечение для телеработы) часто не были на месте, некоторые технологии пришлось быстро внедрять без надлежащего тестирования(что повышает требования к персоналу технической поддержки), и что другие важные проблемы, такие как семейные обязательства (например, новые требования по уходу за детьми или престарелыми) и благополучие (как психическое, так и физическое), были оставлены без внимания. Эти вопросы были особенно актуальны, учитывая общее усиление негативного воздействия на

психическое здоровье, безопасность работы и финансы в связи с пандемией.

Риски и угрозы безопасности

Кибербезопасность была одной из основных проблем во время пандемии, поскольку компании спешно переходили на новые технологические платформы для удаленной работы (и удаленного доступа к корпоративным системам) и делового взаимодействия.

Злоумышленники отслеживали различные проблемы вызванные удаленной работой, а также общей пандемией, чтобы увеличить разнообразие и количество атак.

Риски и уязвимости распределены по двум основным направлениям:

1. Риски безопасности, связанные с сотрудниками, работающими удаленно.

2. Риски, связанные с технологиями, которые были использовались во время пандемии.

1. Риски безопасности, связанные с сотрудниками, сосредоточены на тех проблемах, которые могут быть вызваны (преднамеренно или непреднамеренно) сотрудником.

Основные риски:

- Повышенная вероятность стать жертвой кибератаки из-за отсутствия концентрации или отвлекающих факторов, вызванных домашней работой.

Это может быть связано с семейными обязанностями или бытовыми потребностями, появившимися в связи с пандемией.

- Отсутствие обучения по вопросам безопасности удаленной работы, что приводит к неэффективным методам обеспечения безопасности.

Это повышает вероятность компрометирующей кибератаки. Многие организации не смогли должным образом обучить сотрудников до того, как они были вынуждены работать из дома.

- Доверенные/недоверенные лица в среде удаленной работы (или в семье) могут использовать новый доступ к корпоративным данным или услугам (например, используя разблокированный ноутбук или телефон, или прослушивание конфиденциального телефонного разговора).

Реальность такова, что эти среды могут быть разделены с неизвестными соседями по квартире или другими людьми, которые могут использовать этот длительный период домашней работы в злонамеренных целях.

- Сотрудники, которые сейчас испытывают минимальный контроль или надзор со стороны руководства

могут использовать эту возможность для кражи конфиденциальной информации у своего работодателя или злоупотребления корпоративными услугами. Это может быть мотивировано ощущаемой незащищенностью рабочих мест в связи с пандемией; периодом, когда многие были

уволены, сокращены или отправлены в отпуск.

2. Риски, связанные с технологиями, которые были использовались во время пандемии.

- Поспешное внедрение технологий в связи с национальным блокированием, что приводит к развертыванию непроверенных или ненадежных технологий.Такие технологии могут не работать плохо, что приводит к тому, что сотрудники начинают использовать потенциально опасные теневые IT-практики, например, не используют виртуальные частные сети (VPN).

- Незнание (или отсутствие навыков) новых технологий удаленной работы(например, Microsoft Teams, Zoom и т.д.), что приводит к ошибкам в использовании и управлении функциями безопасности. Скорость, с которой эти технологиибыли внедрены в связи с пандемией, возлагает техническую нагрузку на людей в то время, когда они и так находятся в стрессовых и напряженных ситуациях.

- Проблемы безопасности при использовании технологий удаленной работы и удаленной связи могут подвергнуть организацию повышенному риску. Как отмечалось выше, спешное внедрение новых платформ для работы во время COVID-19 также подвергло предприятиям целый ряд новых угроз, связанных с такими технологиями. Например, за последний год мы наблюдали несколько атак, направленных на Zoom и Microsoft.

- Преднамеренное или непреднамеренное использование рабочих устройств для решения личных вопросов, в результате чего открывает дополнительные риски для рабочих устройств. Например, использование рабочих устройств для просмотра фильмов на незащищённых веб-сайтах или загрузки вредоносных вложений из личной электронной почты, социальных сетей или игровых сайтов.

- Рабочие устройства могут быть украдены из дома или из среды удаленной работы. Если эти устройства не зашифрованы должным образом, они представляют риск для корпоративных данных и служб. Этот риск возрастает во время пандемии, поскольку преступники знают, что большинство людей работает удаленно и поэтому скорее всего, дома у них будет больше мобильных технологий.

- Сотрудники, возвращающиеся на работу после длительного периода удаленной работы, могут принести зараженные устройства в корпоративную сеть. Домашние сети гораздо чаще вероятность взлома гораздо выше, чем корпоративные сети, и поэтому длительный период удаленной работы, связанный с блокировкой, может увеличить вероятность такого риска.

Как видно из приведенных выше примеров, риски безопасности могут исходить из разных областей.

Угрозы конфиденциальности персональных данных сотрудников.

Потенциальное нарушение неприкосновенности частной жизни сотрудников, вызванное использованием работодателями технологий наблюдения/мониторинга на рабочих местах является угрозой конфиденциальности персональных данных сотрудников.

Это может быть мониторинг нажатия клавиш, экранов и посещаемых веб-сайтов. В некоторых случаях сотрудники могут используют свои собственные технологии (смартфоны, ноутбуки) для удаленной работы, тем самым предоставляя работодателям или компаниям, доступ к огромному количеству личных данных сотрудников.

- Новые формы технологий, появляющиеся во время пандемии и способные отслеживать эмоциональное состояние сотрудников, также могут нарушить неприкосновенность частной жизни.

Например, эмоциональные или психологические данные, если они не будут защищены должным образом, то они могут быть использованы для составления профиля сотрудников в зависимости от их самочувствия и, таким образом, повлиять на трудоустройство или перспективы будущей карьеры.

- Раскрытие личной информации в результате того, как используются технологии удаленной работы и коммуникационных технологий. Например, раскрытие домашнего фона во время видеозвонков или размещение фотографий в Интернете домашних офисов может привести к утечке личных данных, которые в дальнейшем могут быть использованы в качестве основы для киберпреступлений. Это затрагивает распространенную проблему чрезмерного обмена информацией в Интернете и ее связь с киберриском .

Заключение

В ходе анализа статей, выше был выявлен ряд существенных рисков, и важно, чтобы организации проверяли , соответствует ли безопасность требованиям . Важно чтобы организации при введении нового программного обеспечения , также переобучали сотрудников для работы с ним. А также, чтобы переобучение включало навыки минимизации рисков для безопасности при работе удалённо.

Заключение

Для достижения данной цели, в процессе прохождения учебной (по получению первичных профессиональных умений и навыков, в том числе первичных умений и навыков научно-исследовательской деятельности) практики познакомился новыми угрозами и рисками безопасности и конфиденциальности при удалённой работе, а так же с угрозами конфиденциальности персональных данных сотрудников.

Также были изучены требования к написанию отчета по практике. В результате прохождения практики был составлен отчет по практике, соответствующий предъявленным требованиям.

В ходе прохождения практики все задачи были выполнены, а цель достигнута.

Список используемых источников

1) Remote Working Pre- and Post-COVID-19: An Analysis of New Threats and Risks to Security and Privacy ⋆ https://arxiv.org/abs/2107.03907 (дата обращения: 17.07.2021).

2) IBM: IBM Security Work From Home Study (2020), https://newsroom.ibm.com/2020-06-22-IBM-Security-Study-Finds-EmployeesNew-to-Working-from-Home-Pose-Security-Risk (дата обращения: 20.07.2021)

3) Таров Д. А., Тарова И. Н. Технические аспекты обеспечения устойчивости информационной среды организации при удаленной работе сотрудников [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://www.elibrary.ru/download/elibrary_44145530_88.. (дата обращения: 23.07.2021)

4) Особенности защиты информации при удалённом доступе [Электронный ресурс]. – Электрон. дан. – Режим доступа: https://elibrary.ru/item.asp?id=45738072 (дата обращения: 23.07.2021)