Литература:

1. *Чернов С.Н.* Нефть и газ Арктики. Правовые, экологические и социальные проблемы освоения странами Арктического совета богатств Севера. – Петрозаводск: КарНЦ РАН, 2020. – 209 с.

2. *Мамахатов Т.М.* Роль Арктики в обеспечении экономической и национальной безопасности России в современных геополитических и климатических условиях // Электронное сетевое издание «Международный правовой курьер». – 2021. – №. 7. – С. 54-60.

3. Указ Президента РФ от 26 октября 2020 г. № 645 «О Стратегии развития Арктической зоны Российской Федерации и обеспечения национальной безопасности на период до 2035 года». – URL: https://base.garant.ru/74810556/ (дата обращения 13.09.2022).

4. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Управление региональной безопасностью на основе сценарного подхода. – М.: ИПУ РАН, 2014. – 163 с.

DOI: 10.25728/iccss.2022.94.81.051

Рыженко А.А.

Организация системы подготовки сотрудников организаций в сфере противоборства механизмам социальной инженерии

Аннотация: Рассматриваются вопросы моделирования центра обучения и подготовки сотрудников организаций в сфере противоборства современным механизмам социальной инженерии.

Ключевые слова: информационная безопасность, социальная инженерия, кибербезопасность, моделирование

Вопросами противоборства методам социальной инженерии занимаются ведущие научные школы мирового уровня достаточно продолжительное время. Еще в начале двухтысячных годов ряд работ отмечал, что в ближайшем будущем, в связи с усилением контура безопасности в глобальной сети Интернет в целом, атаки злоумышленников будут все чаще перенаправляться на социально-психологические факторы социальной инженерии. Например, в

работе [1] еще в 2005 году задается достаточно молодое на тот момент времени направление исследований, которое впоследствии действительно показало свою эффективность на практике как в судебной системе, так и для подготовки технических специалистов.

Пропуская достаточно продолжительный период также стоит отметить, что количество исследований по каждому определяемому временем направлению атак на социальную среду приобретали целые научные направления, которые впоследствии переносились в учебные материалы для следователей в цифровой среде. Например, в работе [2], датированной 2016 годом, поднимаются и описываются вопросы, связанные с уже популярными методами фишинга с использованием мобильных устройств. За последние 2 года данное направление считается одним из ведущих в сфере противоборства методам социальной инженерии.

Параллельно с мировыми школами в РФ развивались свои направления исследований, тесно связанные с особенностями развития взаимодействия технической и алгоритмической составляющей атак злоумышленников с совершенствующимися с каждым годом методами противоборства. Тем не менее, сразу хочется отметить, что тенденция увеличения в процентном соотношении комплексных атак с целью кражи информации с каждым годом все больше склоняется к популярным методам социальной инженерии. Как следствие в основные фондовые программы государственного уровня по цифровой безопасности самым большим разделом является именно противоборство психологическим атакам злоумышленников. В результате с каждым годом появляется все больше информационных материалов и курсов повышения квалификации для различных слоев населения, помогающие социальной среде больше узнать о возможных методах хищения информации.

С другой стороны, ежедневно обновляемые доски объявлений в сети DarkNet, где можно купить практически любую информацию, до сих пор говорят о низкой подготовленности сотрудников многих организаций к действиям злоумышленников. Запредельное доверие мобильным устройствам, социальным сетям, мессенджерам и прочим программно-аппаратным устройствам существенно усложняет специалистам в сфере информационной безопасности профессиональную деятельность: требования не выполняются,

инструкции, лицензии и соглашения не читаются. Например, достаточно частый опрос разных групп в социальных сетях «Читали ли они пользовательское соглашение?», более 90 % опрошенных честно отрицательно отвечали, а около 40 % даже не знали, что такой документ существует.

В качестве нового инструмента возможно воздействие на социальную среду на официальном информационном ресурсе Роскомнадзора предложена модель персональной безопасности, где предлагается каждому подумать о собственном поведении в цифровой среде и разработать индивидуальный контур безопасности вполне официально. Но достаточно неэффективная рекламная кампания данного документа уже продолжительное время не показывает результаты предложенной модели.

В данных исследованиях было решено рассматривать действия злоумышленников не как независимая система воздействия на социальную среду, а как деструктивный постоянно изменяющийся элемент жизненного цикла произвольной существующей системы. В основу модели заложена концепция вируса полиморфика, предложенная еще в 2000 году одним из основателей глобальной сети Интернет. Первые результаты моделирования были представлены ранее в работах [3, 4].

Как было уже упомянуто ранее, полученные результаты переносились в учебные пособия для специалистов судебной системы цифровой среды. В результате, было предложено разработать концепцию единого центра подготовки сотрудников организаций к действиям злоумышленников методами социальной инженерии. Т.е. особенностью данного центра является синтез двух существующих направлений исследований: с одной стороны, – создание унифицированных методик противоборства в информационной среде, с другой, – формирование индивидуальных траекторий обучения, подготовки и самодиагностики для каждого профиля обучаемых. Имеющийся на тот момент опыт организации потоков информации для обучаемых [5] позволил сформировать единую модель формирования поля решений или поля индивидуальных траекторий, включающую бикубическую матрицу «атака – блокировка», иерархическое дерево сквозного проекта комплексной защиты и пирамидальное представление области знаний с фасетными уровневыми основаниями. Сразу стоит

отметить, что аналогичные исследования проводятся и на мировом уровне. Например, в работе [6] представлена аналогичная модель, позволяющая сформировать новый метод, который использует свойства обнаружения сообщества и концепции анализа социальных сетей. В статье показано, что самая высокая производительность достигается, когда функции уровня сообщества и функции социальных сетей используются в сочетании с функциями уровня класса вредоносного ПО, т.е. также строится бикубическая матрица, где связи между ячейками формируются деревом событий.

Помимо того, что в персональном клиенте для каждого обучаемого сотрудника подбираются материалы, повышающие квалификацию, система также работает в активном режиме как консультант к возможным действиям в реальном времени. Пример работы всей системы представлен далее.

В основе модели используется сетевая структура семантической сети с единым центром. Ядром системы выступает база правил, где интерпретатор строит правую часть продукционных правил на основе кратности процессов. Данный принцип достаточно подробно освещался в работах, посвященных операциям над процессами мультимножеств. Особенностью является неоднозначность решения, где после знака равно не одно конкретное решение, а множество решений. Выбор конкретного значения предоставляется агенту посреднику сети баз ассоциаций по адаптивному критерию. Например, звонок клиенту банка с известного номера технической поддержки. Агент поддержки обучаемого в виде мобильного приложения знает контрольные номера. Открывается сессия «дежурства». Так как любая речь мгновенно может быть переведена в текст, то агент сравнивает слова звонящего с внешней базой токсичного контента. Как только попадаются ключевые фразы, агент предлагает абоненту произвести проверку и сделать встречный вызов на тот же номер поддержки. Современные устройства позволяют удержать звонок и вызвать другого абонента. В то же время агент делает обращение на сервер на занятость портов обращения. В результате, даже если абонент откажется делать вызов поддержки, агент покажет достоверную информацию по открытой сессии, т.е. откуда сейчас происходит звонок. К сожалению, не удалось избежать парадоксов и коллизий. В случае одноранговых

процессов, текущая версия агента предлагает пользователю самостоятельно сделать выбор между возможными альтернативами.

Первые результаты работы полученной модели были представлены в работе [7], где изложен конкретный пример учета множественных параметров одного из направлений социальной инженерии при подготовке технических специалистов конкретной сферы профессиональной деятельности. По результатам конференции предложено более детально охватить и другие направления финансовых организаций, но в первую очередь – расширить перечень функционала для банковской сферы.

Литература:

1. *Bénichou D., Lefran S.* Introduction to Network Self-defense: technical and judicial issues // Journal in Computer Virology. – 2005. – Vol. 1. – P. 24-31. DOI: 10.1007/s11416-005-0006-5

2. *Mun H.J., Han K.H.* Blackhole attack: user identity and password seize attack using honeypot // Journal of Computer Virology and Hacking Techniques. – 2016. – Vol. 12. – P. 185-190. DOI: 10.1007/s11416-016-0270-6

3. *Рыженко А.А.* Модель деструктора-полиморфа цифровой среды / Проблемы управления безопасностью сложных систем: материалы XXVI Международной научной конференции (19 декабря 2018 г., Москва). – М.: ИПУ РАН, 2018. – С. 158-162.

4. *Рыженко А.А.* Модифицированный алгоритм вируса полиморфика как основа деструктора информационной среды / Информатика: проблемы, методология, технологии: сборник материалов XVIII международной научно-методической конференции: в 7 т. (Воронеж, Воронежский государственный университет, 14-15 февраля 2019 г.) – Воронеж: Издательство «Научно-исследовательские публикации» (ООО «Вэлборн»), 2019. – Т. 5. – С. 857-861.

5. *Рыженко А.А.* Использование пирамидального образа аналитического мышления при подготовке комплексных решений на примере системы координации ресурсов информационного поля цифровых данных / Информационно-аналитическое обеспечение профессиональной деятельности: материалы межд. научно-практической конференции от 15 мая 2018 г. – М.: МПИ ФСБ России, 2020. – С. 106-116.

6. *Reddy V., Kolli N. & Balakrishnan N.* Malware detection and

classification using community detection and social network analysis // Journal of Computer Virology and Hacking Techniques. – 2021. – Vol. 17. – P. 333-346. DOI: 10.1007/s11416-021-00387-x

7. *Рыженко А.А., Рыженко Н.Ю.* Безопасность информации цифровой экономики / Актуальные проблемы и перспективы развития экономики. Труды Юбилейной XX Всероссийской с международным участием научно-практической конференции. – Симферополь: Издательский дом КФУ, 2021. – С. 289-291.

DOI: 10.25728/iccss.2022.61.83.052

Кротова М.В.

Качественные подходы к моделированию стратегий импортозамещения на отраслевом и межотраслевом уровнях

Аннотация: Импортозамещение является одним из стратегических приоритетов развития национальной экономики РФ в сфере обеспечения собственно защищенности страны от экономических демаршей со стороны компаний и правительств недружественных государств. Это один из редких случаев, когда задачи безопасности не только сдерживают процессы экономического развития, но и непосредственно обеспечивают рост и усложнение структуры ВВП, в его части, находящейся под национальным контролем. На уровне отдельного предприятия-изготовителя стратегия импортозамещения может быть достаточно четко определена в части изменения номенклатуры выпуска. На уровне более крупных хозяйственных комплексов (различного масштаба и структуры) выработка импортозамещающей стратегии может быть представлена как оптимизационная задача с различными наборами критериев оптимизации.

Ключевые слова: экономическая безопасность, технологический суверенитет, импортозамещение, концептуальная независимость, ГИСП