УДК 004.056

ВЛИЯНИЕ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ НА УРОВЕНЬ ТЕХНОСФЕРНОЙ БЕЗОПАСНОСТИ

Л.Г. Основина, К.И. Давыдович, Е.А. Иванов
Белорусский государственный университет информатики и радиоэлектроники, Минск

В мире постоянно появляются и исчезают новые понятия и подходы. На текущем этапе научно-технического прогресса деятельность человека, направленная на повышение комфортности существования, одновременно становится потенциальным источником формирования многочисленных вредных и опасных факторов новой антропогенной среды обитания. В этой связи личная и общественная безопасность перестает касаться исключительно специалистов-профессионалов и становится насущной проблемой каждого человека. Стоящая перед обществом задача рационального и продуманного формирования техносферы, обеспечивающей приемлемые для человека и природных экосистем условия существования, исключительно сложна.

Транспортный комплекс – это совокупность транспортных средств, инфраструктуры и организаций, которые обеспечивают передвижение грузов и пассажиров. Он включает в себя такие элементы, как дороги, порты, аэропорты, автобусные и железнодорожные станции, железные дороги, а также компании, занимающиеся перевозками и логистикой. Главной задачей транспортного комплекса является обеспечение потребностей экономики и населения в перевозках, а также развитие торговых и экономических связей между различными регионами и странами.

Современный уровень промышленной безопасности имеет устойчивый вектор на цифровизацию и возможность применения различных средств дистанционного мониторинга действительного состояния технических устройств и производственных процессов на опасных производственных объектах. Техносферная безопасность существует для защиты окружающей среды от воздействия человека [1]. Современная эпоха характеризуется быстрым промышленным развитием, в результате чего производственные предприятия широко взаимодействуют с природной средой. Люди сталкиваются с экологическими проблемами, и чем больше развивается человечество, тем сильнее негативное воздействие на окружающую среду [2].

Уровень техносферной безопасности в транспортном комплексе определяется мерами, принимаемыми для защиты технических систем и инфраструктуры от различных угроз и рисков. Техносферная безопасность включает в себя защиту от техногенных катастроф, аварий, сбоев и других негативных событий, которые могут повлиять на работу транспортных средств и инфраструктуры. Социальная инженерия представляет серьезную угрозу для транспортных комплексов, так как она основывается на манипуляции и обмане людей для получения несанкционированного доступа к информации или ресурсам транспортного комплекса [3].

Техносферой является часть биосферы, преобразованная людьми с помощью прямого или косвенного воздействия технических средств в целях наилучшего соответствия социально-экономическим потребностям человечества (города, поселения, промышленная зона и др.).

Процессом обеспечение техносферной безопасности является создание и поддержание техносферного пространства в качественном состоянии, исключающем его негативное влияние на человека и природную среду. Данный процесс состоит из таких систем, как производственная безопасность, экологическая безопасность, информационная безопасность, безопасность в чрезвычайных ситуациях др.

Управление техносферной безопасностью представляет собой сложный процесс, который включает в себя оценку рисков, разработку мер по предотвращению рисков, контроль за выполнением мер безопасности, обучение и информирование персонала, расследование и учет инцидентов, а также разработку и внедрение новых технологий и методов обеспечения безопасности. Этот процесс является непрерывным и циклическим, так как на каждом этапе происходит сбор и анализ информации, принятие решений и корректировка действий.

Социальная инженерия – это метод манипуляции людьми с целью получения незаконного доступа к информации или системам, нарушения безопасности или проведения других вредоносных действий. В широком смысле под это понятие подпадают любые ситуации, в рамках которых преступники играют на особенностях человеческой психики и манипулируют индивидами так, чтобы они нарушили обычные процедуры и протоколы безопасности. Злоумышленники не пытаются проникнуть в корпоративную сеть через системные уязвимости, их атаки направлены на людей, которые сами делятся конфиденциальной информацией, что дает доступ в офисные помещения, системы или сети [4].

Атака с помощью социальной инженерии – это форма взлома, при которой злоумышленник пытается получить доступ или информацию, используя доверие. Данная атака является очень эффективной, поскольку она использует желание человека помочь другим людям. Социальный инженер использует манипуляции высокого уровня для получения необходимой ему информации. Это одна из форм хакерства, но вместо взлома компьютеров социальные инженеры пытаются получить к ним доступ, обманом заставляя сотрудников выдать информацию или загрузить вредоносное ПО.

Атака социальной инженерии как правило начинается с исследования цели и ее окружения. Злоумышленник может собирать информацию о цели из различных источников, таких как социальные сети, общественные базы данных или наблюдая за поведением цели в общественных местах. Затем злоумышленник создает сценарий, который позволит ему манипулировать целью. Например, фальшивый звонок от представителя компании, требующий от цели предоставить конфиденциальную информацию или выполнить определенные действия. Злоумышленник может использовать знание об окружении цели, чтобы создать иллюзию легитимности и убедить ее в необходимости действовать. Он может использовать такие методы манипуляции как угрозы, обещания или создание ситуации, в которой цель чувствует себя обязанной помочь [5]. В результате успешной атаки злоумышленник получает доступ к конфиденциальной информации, финансовым ресурсам или физическим объектам. В некоторых случаях, атака может быть незаметной для цели, и злоумышленник может продолжать получать доступ к информации или ресурсам в течение продолжительного времени.

Самым популярным видом социальной инженерии на сегодняшний день является фишинг. Фишинговые атаки нацелены на мошенническое получение частной и конфиденциальной информации от предполагаемых целей с помощью телефонных звонков или электронной почты. Злоумышленники вводят жертв в заблуждение, чтобы получить конфиденциальную информацию. Они включают в себя поддельные веб-сайты, электронные письма, рекламу, антивирус, вредоносное программное обеспечение, бонусы и бесплатные предложения. Атакой может быть звонок или электронное письмо от поддельной лотереи о выигрыше с запросом личной информации или необходимостью нажатия на ссылку, прикрепленную к письмам. Полученная информация может

являться данными кредитной карты, страховыми данными, полным именем, физическим адресом, первой работой или работой мечты, именем матери, местом рождения, посещенными местами или любой другой информацией, которую человек может использовать для входа в конфиденциальные учетные записи.

Не менее опасным является такой вид атаки, как вишинг – это разновидность кибер-преступлений, направленных на кражу личной информации по телефону. Под вишингом подразумевается вид мошенничества, при котором преступники, охотящиеся за персональной или финансовой информацией жертвы для использования в корыстных целях против нее, используют телефон, чтобы в телефонной беседе попытаться заполучить требуемые данные. Злоумышленники, использующие технику вишинга, обычно проводят подмену номера, с которого осуществляется звонок, в результате чего жертва думает, что телефонный звонок является местным (город или регион жертвы) и от существующей организации. Злоумышленники выдают себя за официальное лицо какой-либо легальной компании или организации, пытаясь обманным путем заставить жертву предоставить свою персональную информацию. Одним из самых распространённых случаев является представление себя за сотрудника банка. Когда потенциальная жертва поднимает трубку телефона, мошенники создают ощущение срочности, чтобы сыграть на ее эмоциях и заставить ее действовать требуемым образом, чтобы предоставить персональную информацию. Преступники могут сказать, что наблюдается проблема с одним из финансовых счетов, которая должна быть немедленно устранена. Вишинг может принимать различные формы, но цель он всегда имеет единственную цель: обманом заставить человека раскрыть конфиденциальную информацию, будь то для получения финансовой выгоды или для совершения другого преступления, такого как кража регистрационных данных или онлайн-личности. Простейшим способом избежания вишинговой атаки является уход от ответа на телефонные звонки с неизвестных номеров телефонов.

На ряду с фишингом и вишингом выделяется такой тип атак, как смишинг. Смишинг – это разновидность кибер-преступлений, осуществляемая посредством отправки поддельных SMS-сообщений или звонков на мобильные телефоны с целью получения конфиденциальной информации или финансовых данных. Основной целью смишинга является мошенническое получение денежных средств либо конфиденциальной информации от пользователей. Злоумышленники зачастую притворяются представителями банков, компаний или сервисов социальных сетей, чтобы вызвать доверие у получателя сообщения и убедить его в необходимости выполнить определенные действия. Смишинг может проявляться в виде: подделки доставки, где злоумышленники могут отправить SMS-сообщение, выдающееся за уведомление от курьерской службы, с просьбой подтвердить доставку путем предоставления личных данных или оплаты дополнительных сборов, фальшивых уведомлений банков, в которых злоумышленники могут отправить SMS-сообщение, выдающееся за уведомление от банка, с просьбой предоставить логин и пароль для проверки аккаунта или обновления информации, фальшивых лотерей или акций, где злоумышленники могут отправить SMS-сообщение, обещающее выигрыш в лотерее или участие в акции, с просьбой предоставить личные данные или оплатить комиссию для получения приза. Для защиты от смишинга важно быть осторожным при получении SMS-сообщений от неизвестных отправителей или с подозрительным содержанием. Не следует предоставлять личную информацию или выполнять нежелательные действия в ответ на такие сообщения. При появлении подозрений, необходимо связаться с официальным представителем банка или организации, от имени которой было отправлено сообщение, для проверки его подлинности.

Для рядовых пользователей самый актуальный и действенный способ уклониться от социальной инженерии – всегда оставаться бдительными, проверять информацию об отправителе, прежде чем перейти по ссылке или скачать предлагаемый файл — убедиться, что это не вредоносный ресурс. Полученные файлы перед открытием необходимо проверять с помощью антивирусного ПО. Стоит также удостовериться, что домен отправителя легитимный и реальный. В случае возникновения сомнений, необходимо проверить, действительно ли адресат отправлял данное письмо и является ли он настоящим владельцем электронного ящика, связавшись с ним каким-либо альтернативным способом, например, через мессенджер или по телефону. Своевременное выявление и пресечение атаки позволяет избежать серьезных последствий.

Рассмотрим возможные проявления социальной инженерии в транспортном комплексе.

1. Фальшивые проверки безопасности. Злоумышленник может притвориться сотрудником службы безопасности и провести фальшивую проверку на входе в транспортный комплекс. В ходе этой проверки он может попросить жертву предоставить личную информацию, такую как пароль

или пин-код, или даже передать ему запрещенные предметы. Полученная информация может быть применена для получения доступа к системам или ресурсам компании.

2. Фальшивые поставщики или клиенты. Злоумышленник может притвориться поставщиком или клиентом компании, чтобы получить доступ к офису или складу. Он может использовать этот доступ для кражи информации о клиентах, товарах или других конфиденциальных данных. Злоумышленник может также использовать свой статус для проведения фальшивых сделок или заказов, которые могут привести к потере ресурсов или финансовых убытков.

3. Маскировка под сотрудника. Злоумышленник может притвориться сотрудником транспортной компании, используя подходящую форму одежды или аксессуары, такие как жилет с логотипом компании или фальшивый пропуск. Он может воспользоваться этим статусом для получения доступа к ограниченным зонам, таким как склады или офисы, где хранятся конфиденциальные данные или ценные ресурсы.

4. Фальшивые ремонтные работы. Злоумышленник может представиться работником по ремонту или обслуживанию транспортных средств и предложить свои услуги. В ходе этих работ он может получить доступ к внутренним системам или украсть конфиденциальную информацию. Злоумышленник может также использовать эту возможность для установки устройств слежения или вредоносного программного обеспечения на транспортные средства компании.

5. Фальшивые заявки на доставку. Злоумышленник может отправить фальшивую заявку на доставку груза, притворяясь клиентом или поставщиком. Он может использовать эту схему для получения доступа к складу или для кражи груза. Также возможно использование фальшивых документов или поддельных идентификационных данных, чтобы убедить сотрудников в подтверждении доставки или передачи груза.

6. Подделка информации о рейсе. Злоумышленники могут отправить SMS-сообщение с измененной информацией о времени вылета или прибытия рейса, с целью создать панику у получателя и получить от него личные данные или оплату за изменение бронирования.

7. Фальшивые уведомления о задержке рейса. Злоумышленники могут отправить SMS-сообщение, утверждая, что рейс задерживается или отменяется, и просить получателя предоставить личные данные или оплатить дополнительные сборы для перебронирования на другой рейс.

Для снижения риска социальной инженерии надо придерживаться базовым правилам:

– никому не сообщать логины и пароли от своих учётных записей;
– не скачивать вложения и не переходить по подозрительным ссылкам в электронных письмах;
– блокировать компьютер, уходя от своего рабочего места;
– использовать надежные и уникальные пароли для различных сервисов.

Для предотвращения социальной инженерии следует обучать сотрудников так, чтобы они могли с лёгкостью распознавать признаки социальной инженерии, а также знать методы предотвращения атак. Обучение должно включать основы безопасности, распознавание фальшивых проверок или запросов на информацию, а также стратегии общения с посетителями и клиентами. Стоит установить строгие процедуры проверки личности для всех посетителей, поставщиков и клиентов, а также для сотрудников компании. Для этого могут применены такие методы, как использование многофакторной аутентификации, проверку документов, и других технических средств для обеспечения безопасности доступа к ограниченным зонам или информации.

Строгая политика безопасности также является одним из ключевых факторов для предотвращения социальной инженерии. Сотрудники должны быть ознакомлены с процедурами, которые необходимо выполнить для обработки запросов на изменение платежных данных, бронирования рейсов. Важно установить ясные правила и требования для проверки подлинности запросов и подтверждения легитимности клиента.

Контролировать доступ к информации можно установив системы контроля доступа, такие как электронные пропускные системы или видеонаблюдение, чтобы отслеживать и регистрировать все посещения и перемещения внутри транспортного комплекса, что позволит быстро выявлять подозрительную активность и принимать меры по ее предотвращению. Также следует установить системы защиты информации, такие как брандмауэры, антивирусные программы, системы обнаружения вторжений и шифрование данных. Это поможет предотвратить несанкционированный доступ к ценной информации и защитить ее от утечек. При выявлении подозрительной активности следует как можно быстрее сообщать сотрудникам и клиентам о возможных угрозах социальной инженерии и предоставлять рекомендации по безопасности, для этого требуется регулярно обновлять политику безопасности компании и обеспечивать ее соблюдение.

Важным аспектом также является обеспечение физической безопасности. Обеспечить физическую безопасность транспортного комплекса возможно, включая установку ограждений, видеонаблюдения, освещения и других мер, которые помогут предотвратить несанкционированный доступ. Требуется проводить регулярные аудиты безопасности, чтобы выявлять уязвимости и проблемы в системах безопасности транспортного комплекса. Это позволит своевременно принимать меры по устранению уязвимостей и повысить общий уровень безопасности.

Подводя итог можно сказать, что социальная инженерия представляет серьезную угрозу для транспортных комплексов, но с помощью правильных мер безопасности и обучения сотрудников, риски можно значительно снизить.

Ключевым является обучение сотрудников и повышение их осведомленности о методах социальной инженерии, строгие процедуры проверки личности и доступа, системы контроля доступа, повышение физической безопасности и установка систем защиты информации, но не стоит забывать о том, что социальная инженерия может применяться не только в отношении персонала транспортного комплекса, но и в отношении клиентов и пользователей, поэтому необходимо обеспечить безопасность их личных данных. Требуется создать культуру безопасности в транспортном комплексе, где каждый сотрудник осознает свою ответственность за сохранность конфиденциальной информации и знает, как действовать в случае подозрительных ситуаций. Регулярные аудиты безопасности также помогут выявить уязвимости и проблемы в системах безопасности и принять меры по их устранению.

Таким образом социальная инженерия является серьезной угрозой для транспортных комплексов, поскольку она может привести к утечке конфиденциальной информации, финансовым потерям и нарушению безопасности клиентов и сотрудников. Однако, важно понимать, что социальная инженерия постоянно развивается, поэтому необходимо постоянно обновлять и усовершенствовать меры безопасности, чтобы быть на шаг впереди злоумышленников.

Список использованных источников

1. Белов С.В. Безопасность жизнедеятельности и защита окружающей среды (техносферная безопасность): учебное пособие / С. В. Белов. – 5-е изд., пер. и доп. – Москва : Юрайт, 2017. – 350 с.

2. Русаков, А. Ю. Понятие информационной безопасности для студентов направления подготовки «техносферная безопасность» / А. Ю. Русаков // Неделя науки СПбПУ : материалы научной конференции с международным участием, Санкт-Петербург, 19–24 ноября 2018 года.

3. Определение социальной инженерии // Безопасность через образование : [Электронный ресурс]. – Режим доступа: https://www.social-engineer.org/framework/general-discussion/social-engineering-defined– Дата доступа: 17.10.2023.

4.Социальная инженерия в контексте информационной безопасности: понятие, виды, значение // Следственный комитет Республики Беларусь: официальный сайт. [Электронный ресурс]. – Режим доступа: https://sk.gov.by/ru/news-ru/view/sotsialnaja-inzhenerija-v-kontekste-informatsionnoj-bezopasnosti-ponjatie-vidy-znachenie-10991/– Дата доступа: 18.10.2023.

5.Аргамакова, А. А. Прикладное социогуманитарное знание, социальные технологии и инженерия / А. А. Аргамакова // Epistemology & Philosophy of Science. – 2015. – Vol. 46, No. 4. – P. 70-84.