ОБУЧЕНИЕ КАК ПРОТИВОДЕЙСТВИЕ МЕТОДАМ СОЦИАЛЬНОЙ ИНЖЕНЕРИИ

DOI: 10.25629/HC.2021.03.15

Останина Е.А.

Московский авиационный институт (национальный исследовательский университет)

Аннотация. Изучение вопросов защиты информации является одной из важнейших проблем современного мира. Актуальность данной темы неразрывно связана с постоянным развитием информационных технологий и повсеместным использованием электронных документов. Безопасность информации в информационной системе, включая телекоммуникационные сети, может быть обеспечена только комплексным применением методов и средств защиты. Наиболее уязвимым звеном в этой системе может быть признан человек. Используемые при этом методы атак, как правило, направлены на формирование такой поведенческой модели человека (работника), которая выгодна злоумышленнику и носит ложное представление о добровольности и самостоятельности ее принятия объектом воздействия. Применяемые техники социальной инженерии основаны на личностных особенностях и их учете при принятии решений человеком. Важно отметить, что такие методы достаточно эффективны, просты и дешевы в реализации, а также имеют невысокую степень риска. В статье приведены данные, характеризующие долю воздействия такими методами на физических и юридических лиц. В России методы социальной инженерии получили достаточно широкое распространение, и их доля значительно возросла в связи с ростом проведения удаленных платежных операций, пересылкой электронных документов и увеличением онлайн-услуг в период пандемии.

Основным способом защиты от социальной инженерии, по многочисленным утверждениям ученых и работодателей, является обучение. Проведенное исследование, в ходе которого был проведен опрос обучающихся по вопросам информационной безопасности, а также было предложено решить кейсы с ситуациями нарушения информационной безопасности посредством применения злоумышленником технологий социальной инженерии, показал низкий уровень подготовленности. Не было выявлено значительных различий и в группах обучающихся по различным направлениям подготовки. Выявлена целесообразность корректировки программ.

Ключевые слова. Информационная безопасность, социальная инженерия, подготовка обучающихся, методы противодействия мошенникам, персональные данные, коммерческая тайна, угроза безопасности.

Введение

В настоящее время в ответ на современные вызовы разработан ряд методов и средств защиты информации. Как правило, к ним в первую очередь относят техническую и программную составляющие защиты. Говоря о технической защите информации, предполагают защиту информации, заключающуюся в обеспечении безопасности информации (данных), подлежащей защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств, не криптографическими методами [3]. Также в вопросах обеспечения информационной безопасности важная роль отводится законодательным и организационным методам защиты информации.

Любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность, принято называть инцидентом информационной безопасности. К таковым могут быть отнесены: утрата услуг, оборудования или устройств; системные сбои или перегрузки; ошибки пользователей; несоблюдение политики или рекомендаций по информационной безопасности; нарушение физических мер защиты; неконтролируемые изменения систем; сбои программного обеспечения и отказы технических средств; нарушение правил доступа к информационным ресурсам [4].

Краткий анализ литературы

Анализ научной литературы по вопросам, описывающим арсенала основных средств, применяемых в социальной инженерии в совокупности с данными исследований крупных компаний (Центрального банка РФ, автономной некоммерческой организации «Российская система качества», Fortinet, информационного портала по безопасности SecurityLab.ru и других), а также различных программ подготовки обучающихся показал актуальность изучения методов и способов защиты от социального хакерства. Подчеркивается, что в современном мире информационная безопасность выходит на первый план и трата на ее техническую защиту огромных денег не всегда приносит желаемый результат. Ключевым фактором становится готовность человека противостоять социальной инженерии, однако в настоящее время соответственная подготовка в рамках программ среднего специального и высшего образования по всем направлениям подготовки не достаточна либо отсутствует.

Обсуждение вопроса

В рамках данной статьи особое внимание уделим человеческому фактору, полагая его наиболее уязвимой составляющей информационной безопасности в сложившихся условиях деятельности компаний, организаций и государственных структур. Также при рассмотрении вопросов сосредоточимся на работе сотрудников со сведениями, не содержащими государственную тайну, но имеющими отношение к персональным данным граждан или содержащим коммерческую тайну.

Пожалуй, именно взаимодействие человека с элементами информационной системы таит в себе наибольшую угрозу в наше время. Постоянное совершенствование информационных технологий и обеспечивающих их технических средств способно сыграть злую шутку даже с добросовестным работником. Угрозу может нести как преднамеренное действие сотрудника, так и совершенное по неосторожности, по незнанию (не достаточной квалификации сотрудника), а, возможно, и при непосредственном воздействии на него методами социальной инженерии.

Безусловно, злоумышленник может попытаться завладеть информацией путем осуществления взлома базы данных, перехвата сообщений или документов в сети, съема информации с технических устройств (мониторов, клавиатур, принтеров) и каналов передачи данных, а также предпринять попытку модификации или уничтожения информации. Однако, в данной статье основное внимание будет уделено другому методу, который известен как социальная инженерия. В связи с этим, целесообразно подробнее рассмотреть достаточно эффективный метод получения конфиденциальной информации и информации, содержащей коммерческую тайну, который во многом основан на использовании слабостей, предрассудков и комплексов человеческого ресурса организации.

В современной интерпретации англоязычный термин «social engineering» можно представить как целостную группу психологических и аналитических приемов воздействия на сотрудников с целью «подталкивания» их к совершению действий, ведущих к нарушению информационной безопасности.

При этом используемые методы направлены на формирование такой поведенческой модели работника, которая выгодна злоумышленнику и носит ложное представление о добровольности и самостоятельности ее принятия объектом воздействия. В этой связи часто используется такое понятие как аттракция, обозначающее возникновение при восприятии человека человеком привлекательности одного из них для другого [7].

Как правило, все техники социальной инженерии основаны на личностных особенностях и их учете при принятии решений человеком. Важно отметить, что такие методы достаточно эффективны, просты и дешевы в реализации, а также имеют невысокую степень риска [9]. Целесообразно обратить внимание на следующие из них.

Претекстинг, предполагающий некое действие, отработанное по заранее составленному сценарию (претексту), в результате чего человек должен совершить определённое действие или раскрыть информацию. Заблаговременная подготовка позволяет выяснить некоторые сведения об объекте воздействия. Например, имя сотрудника, его должность, круг интересов и

знакомств. В дальнейшем эти фрагменты могут быть встроены в разговор, как правило, телефонный, для обеспечения доверия объекта воздействия.

Техника, направленная на неправомерное получение конфиденциальной информации, когда злоумышленник подделывает официальное письмо, в котором предполагается «проверка» какой-либо информации или совершение определенных действий, называется фишинг. Как правило, такое письмо содержит ссылку на поддельную, имитирующую оригинал, web-страницу, которая предполагает введение конфиденциальной информации, вплоть до пин-кода банковской карты, паролей корпоративной сети и т.д.

Техника «Троянский конь» основана на чувствах любопытства или алчности людей в совокупности с невнимательностью [1]. При необдуманном «клике» пользователя на вложение в письме злоумышленник достигает своей цели, а именно добавляет эксплойт – подвид вредоносной программы, содержащей данные или исполняемый код, способный воспользоваться одной или несколькими уязвимостями в программном обеспечении на локальном или удаленном компьютере.

Метод атаки «Дорожное яблоко» является вариацией троянского коня, предполагая уже использование физического носителя информации, например, флеш-носителя (с логотипом компании, интригующей подписью или даже без таковых). При подключении такого устройства запускается вредоносная программа и конфиденциальная информация, хранящаяся на компьютере, передается злоумышленнику по сети, либо модифицируется (шифруется) или уничтожается.

Квипрокво (лат. qui pro quo – недоразумение, заключающееся в том, что одно лицо, понятие или вещь оказывается принятым за другое). В этом случае злоумышленник выдает себя по телефону за сотрудника компании, например, представителя техподдержки и в результате «устранения проблем» или загрузки обновлений внедряет команды, позволяющие запустить вредоносное программное обеспечение.

Отдельно стоит выделить такое явление как обратная социальная инженерия, которая предполагает самостоятельное обращение человека за «помощью» к злоумышленнику. Это достигается проведением рекламных или диверсионных операций, например, созданием обратимой неполадки на компьютере жертвы с последующей рекомендацией (демонстрацией визитки, советом хорошего знакомого) обратиться при таких проблемах к злоумышленнику по указанным координатам [10]. Отмечается, что фишинг может стать более локальным, направленным на конкретного человека через социальные сети и мессенджеры. [5]

Это далеко не полный перечень возможных жизненных ситуаций и предполагает постоянный мониторинг подобных инцидентов и включения разбора их в процесс обучения по вопросам информационной безопасности.

Рядом специалистов отмечается, что в России методы социальной инженерии получили достаточно широкое распространение. По сравнению с другими странами эта проблема «нарастает со взрывной скоростью» [16]. В докладах Центрального банка и в комментариях компаний в сфере информационной безопасности обозначаются при этом две причины такого роста: низкая киберграмотность граждан и практически регулярные утечки баз данных из госструктур и коммерческих организаций.

Рассматривая социальные сети и многочисленные форумы как источник информации, следует отметить, что пользователи не всегда заботятся о безопасности аккаунтов, используя простые и идентичные пароли, не проверив надежность ресурса вводят учетные данные и информацию, помогающую при подборе пароля. Этим исследователи объясняют высокую долю украденных учетных данных (44%) в атаках на частных лиц [6].

Так как в настоящее время данные банковских карт и платежная информация клиентов, как правило, защищены криптографическими методами, узнать их проще напрямую у клиента, прибегнув к методам социальной инженерии. Как следствие, порядка 35% украденных данных по банковским картам получены в результате атак на частные лица.

Приведем типизацию украденных данных при атаках на частные и юридические лица. Так, при атаке на юридическое лицо (компанию) учетные записи составляют 27%, персональные данные 29%, данные платежных карт 13%, информация, относящаяся к категории коммерческой тайны 12%, медицинская информация 7%, базы данных клиентов 6%, личная переписка 2%, другая информация 4%. В тоже время при атаке на физическое лицо складывается следующая картина: 44% составляют учетные данные, 7% персональные данные, данные платежных карт 34%, 9% личная переписка и 6% другая информация [6].

Отметим, что использование дистанционных способов оплаты товаров и услуг той частью населения, которая до введения ограничений в связи с пандемией COVID-19 приобретала и оплачивала их непосредственно в точках продаж, привело к росту практически на 40% числа проведенных финансовых операций без согласия пользователей. В силу отсутствия необходимого опыта противодействия злоумышленникам значительная часть наших граждан оказалась уязвима к социальной инженерии. Доля операций, проведенных без согласия пользователей (клиентов) с использованием социальной инженерии за 2019 и 2020 годы [12] представлена в таблице 1.

Таблица 1 – Доля операций, проведенных без согласия пользователей (клиентов) с использованием социальной инженерии

	2019 год				2020 год			
	I квартал		II квартал		I квартал		II квартал	
Операции	Кол-во (ед)	Доля соц. инженерии	Кол-во (ед)	Доля соц. инженерии	Кол-во (ед)	Доля соц. инженерии	Кол-во (ед)	Доля соц. инженерии
Банкоматы, терминалы	8095	30%	9904	22%	11273	13%	9434	15%
Оплата товаров и услуг в Интернете	73819	56%	66957	65%	123617	63%	152857	89%
Система дистанционного банковского обслуживания физлиц	42015	86%	34308	94%	34035	85%	29238	87%
Система дистанционного банковского обслуживания юрлиц	859	5%	2081	8%	576	44%	807	29%

Таким образом, по ряду позиций доля атак с использованием социальной инженерии значительна и достигает значений в 80-90%.

По данным информационного портала по безопасности SecurityLab.ru количество подобных атак в 2020 году выросло на 147% [8].

Третий квартал 2020 года по данным специалистов Центрального банка РФ также показал рост по всем видам атак, за исключением атак с использованием уязвимостей в программном обеспечении.

В 2020 году появилось множество новых схем мошенничества [11]:

в ноябре Роскачество оповестило о новой схеме мошенничества в Telegram, когда злоумышленник обращается к администраторам каналов в мессенджере под видом переговоров о размещении оплачиваемой рекламы и размещает архивный файл с «презентацией» продукта. При этом архив содержит вирус, который позволяет передавать данные и управление аккаунтом хакерам;

в апреле компания Fortinet сообщила о том, что активизировались мошенники, использующие приемы социальной инженерии в период пандемии, характеризующийся повышенной тревожностью и неуверенностью людей;

участились попытки заманивания ничего не подозревающих жертв на зараженные web-сайты, провоцирования перехода по вредоносным ссылкам или предоставления личной информации по телефону.

Отметим, что современные киберпреступники – это эксперты в вопросах маскировки, манипулирования, воздействия и конструирования наживок для обмана людей с целью получения конфиденциальных данных или доступа к сетям и стратегическим объектам организаций.

Как правило, компании тратят огромные финансовые средства на обеспечение информационной безопасности техническими методами, в то время как эти технические средства могут быть бесполезны, если сотрудники не будут знать меры по противодействию социальной инженерии, либо просто пренебрегут ими [13]. Основным способом защиты от социальной инженерии, по многочисленным утверждениям ученых и работодателей, является обучение. Отметим, что это обучение должно проводиться не только работодателем. Основную часть знаний и навыков противодействия должна быть усвоена еще в стенах учебного заведения с последующей их актуализацией. Таким образом, при обучении целесообразно давать знания о потенциальных угрозах и способах получения злоумышленниками конфиденциальной информации, будь то персональные данные или сведения, отнесенные к различным категориям тайн, и способы предотвращения подобных действий.

В процессе обучения следует обратить внимание на обязательность при работе исполнению инструкций компаний. В них, как правило, прописываются вопросы, затрагивающие информационную безопасность компании, как правильно (точно, без ошибок) аутентифицировать собеседника при телефонном общении, как идентифицировать человека и определить его принадлежность к сотрудникам компании, как сопровождать клиентов [2].

В ходе работы по исследованию целесообразности обучения по вопросам информационной безопасности в общем и по вопросам противодействия социальной инженерии был проведен опрос студентов наборов 2018, 2019 и 2020 годов различных направлений подготовки в нескольких вузах города Москвы. В ходе опроса обучающимся предлагалось продемонстрировать свою подготовленность по вопросам информационной безопасности, а также решить кейсовые задачи с ситуациями нарушения информационной безопасности посредством применения злоумышленником технологий социальной инженерии.

В результате выяснилось, что при загрузке файлов только треть из опрошенных проводит оценку надежности ресурса, предоставляющего информацию. При посещении проверенных ресурсов и скачивании программных продуктов только 10% читает пользовательское соглашение. При пересылке сканов документов, в частности, содержащих персональные данные обучающиеся (порядка 90%) практически не заботятся об их программной защите, что может привести к неправомерному использованию этих электронных копий. Безответственно подходят к созданию паролей около 40% респондентов, более ответственно подходят к данному вопросу обучающиеся по техническим направлениям (только около 25% из них используют простые пароли или идентичные для разных ресурсов). Подключение к незащищенным WI-FI осуществляли 30% опрошенных. По признанию респондентов, 16% попадали на уловки мошенников через социальные сети.

В результате решения кейсов установлено, что 27% обучающихся ошиблись при идентификации злоумышленника, посчитав его работником госучреждения, банка, компании. Ошибались при выявлении поддельных сайтов организации и не проявляли осторожности 23% опрошенных, не осуществляли дополнительную проверку – 21%.

При активной деятельности в Интернет-пространстве (социальных сетях, мессенджерах, различных сообществах) у респондентов отмечалась не всегда правильная (адекватная) оценка

собеседников, знакомых возможно только в виртуальном пространстве, и неоправданная доверчивость при затрагивании вопросов о персональных данных и данных конфиденциального характера, относящихся к трудовой деятельности.

Отметим, что участие в различных конкурсных и бонусных программах, требующих согласие на обработку персональных данных, притупляет чувство осторожности людей. Они перестают читать текст данного документа, чем подвергают себя опасности, так как базы, содержащие телефонные номера и другие персональные данные, пользуются большим спросом у недобросовестных рекламодателей и прочих мошенников. Порой, в согласиях на обработку персональных данных, которые в настоящее время подписываются очень часто, присутствует передача данных третьим лицам без указание таковых, не определены цели сбора данных и возможность отзыва согласия.

Также в ходе беседы с обучающимися выяснилось, что 64% из них при сборе персональных (в том числе биометрических) данных в различных организациях, например, в банках при оформлении пластиковой карты, не задумываются о правомерности таких действий, о возможности непредоставления части персональных данных какой-либо организации, не интересуются целями сбора данных и возможностями отзыва согласия на их обработку [14].

Также было отмечено неправильное определение категорийности конфиденциальной информации (в части знания законодательства о персональных данных, о коммерческой и государственной тайнах), а чаще не придание значения последствиям передачи информации третьим лицам.

Обратившись к наименованиям укрупненных групп направлений подготовки, которые приведены в Приложении N 1 к Приказу Министерства образования и науки РФ от 12 сентября 2013 г. N 1061 «Об утверждении перечней специальностей и направлений подготовки высшего образования», невозможно выделить те направления, которые можно было бы исключить из рассмотрения в следствии неактуальности затрагиваемых в исследовании вопросов. В документе определены следующие группы: математические и естественные науки; инженерное дело, технологии и технические науки; здравоохранение и медицинские науки; сельское хозяйство и сельскохозяйственные науки; науки об обществе; образование и педагогические науки; гуманитарные науки; искусство и культура [15]. Во всех этих направлениях в настоящее время активно используются средства вычислительной техники и компьютерные сети, взаимодействие между специалистами происходит посредством локальных и глобальной сетей, а информационные ресурсы «черпаются» из электронных хранилищ библиотек. В тоже время персональные данные сотрудников хранятся в системах электронного документооборота и на государственных порталах различных ведомств.

Выводы

В связи с вышесказанным представляется целесообразным обратить особое внимание на вопросы информационной безопасности при подготовке специалистов различного профиля в организациях среднего профессионального и высшего образования. Для технических направлений подготовки, помимо технической и законодательной составляющей в дисциплине «Информационная безопасность» («Защита информации»), должна обязательно присутствовать тема, посвященная использованию социальной инженерии.

Для прочих направлений подготовки вопросы противодействия методам социальной инженерии целесообразно включить в такие дисциплины, как «Психология», «Социальная психология», «Информатика и информационно-телекоммуникационные технологии», «Информационные технологии» и, возможно, ряд других, так как в настоящее время неправомерное использование персональных данных злоумышленниками может нанести не только материальный вред их обладателю. Даже не осознанной разглашение работником сведений, подпадающих под категорию коммерческой тайны, может привести к материальным потерям компании, а под категорию государственной тайны может поставить под удар безопасность государства.

Заключение

В заключении отметим, что методы социальной инженерии будут активно использоваться и в дальнейшем, возможно уже не только в ныне актуальном контексте (в связи с темой коронавируса), но и в каких-то новых своих проявлениях. Вопрос подготовки людей к противодействию подобным методам будет всегда актуален там, где получение прибыли оправдывает средства.

Библиография

1. Mitnick, Kevin David. The art of deception: controlling the human element of security / Kevin D. Mitnick & William L. Simon. – Indianapolis, Ind.: Wiley, cop. 2002.

2. Siadati, H. Mind your SMSes: Mitigating social engineering in second factor authentication / H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, N. Memon // Computers & Security. – 2017. – Т. 65. – P. 14-28.

3. ГОСТ Р 50922-2006 Защита информации. Основные термины и определения. URL: https://technical_translator_dictionary.academic.ru/239897/техническая_защита_информации (дата обращения: 1.02.2021).

4. ГОСТ Р 53114-2008: Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. URL: http://docs.cntd.ru/document/1200075565 (дата обращения: 1.02.2021).

5. Информационная безопасность в 2021 году. Угрозы, отраслевые тренды. Блог компании ITGLOBAL.COM. URL: https://habr.com/ru/company/itglobalcom/blog/540748/ (дата обращения: 5.02.2021).

6. Исследование. Актуальные киберугрозы II квартал 2019 года. URL: https://ptsecurity.com (дата обращения: 7.02.2021).

7. Карпенко Л.А. Краткий психологический словарь. – Ростов-на-Дону: «ФЕНИКС». Л.А. Карпенко, А.В. Петровский, М.Г. Ярошевский. 1998.

8. Количество атак с использованием социальной инженерии выросло на 147% в 2020 году. URL: https://www.securitylab.ru/news/515178.php: https://www.securitylab.ru/news/515178.php (дата обращения: 11.02.2021).

9. Краткое введение в социальную инженерию. URL: https://habr.com/ru/post/83415/ (дата обращения: 15.02.2021).

10. Кузнецов, М.В. Социальная инженерия и социальные хакеры / М.В. Кузнецов, И.В. Симдянов. – СПб.: БХВ-Петербург, 2007.

11. Обзор TAdviser. Социальная инженерия. URL: https://www.tadviser.ru/index.php (дата обращения: 05.02.2021).

12. Обзор отчетности об инцидентах информационной безопасности при переводе денежных средств I и II кварталы 2019 – 2020 годов. Банк России. URL: https://yandexwebcache.net/yandbtm?lang=ru&fmode=inject&tm=1613241333&tld=ru&la=1612962048&text=статистика%20социальной%20инженерии%202020&url=https%3A%2F%2Fcbr.ru%2Fanalytics%2Fib%2Freview_1q_2q_2020%2F&l10n=ru&mime=html&sign=6e5cb27a99a583ff589c38b7aefc944c&keyno=0 (дата обращения: 11.02.2021).

13. Останина Е.А. Информационная безопасность при реализации концепции BYOD // Человеческий капитал. 2019. № 12 (132). С. 131-141.

14.Останина Е.А. О некоторых аспектах технологии распознавания лиц // Человеческий капитал. 2020. № 5 (137). С. 142-152.

15. Приказ Министерства образования и науки РФ от 12 сентября 2013 г. N 1061 "Об утверждении перечней специальностей и направлений подготовки высшего образования" (с изменениями и дополнениями) Приложение N 1. Перечень направлений подготовки высшего образования – бакалавриата. URL: https://base.garant.ru/70480868/53f89421bbdaf741eb2d1ecc4ddb4c33/ (дата обращения: 12.02.2021).

16. Социальная инженерия в России эффективнее, чем в других странах. URL: https://habr.com/ru/news/t/459278/ (дата обращения: 15.02.2021)

Останина Елена Анатольевна. E-mail: neka1818@mail.ru

LEARNING AS AN OPPORTUNITY TO SOCIAL ENGINEERING

DOI: 10.25629/HC.2021.03.15

Ostanina E.A.

Moscow Aviation Institute (National Research University)

Abstract. The study of information security issues is one of the most important problems of the modern world. The relevance of this topic is inextricably linked with the constant development of information technology and the widespread use of electronic documents. Information security in the information system, including telecommunication networks, can only be ensured by the complex application of methods and means of protection. The most vulnerable link in this system can be recognized as a person. The methods of attacks used in this case, as a rule, are aimed at the formation of such a behavioral model of a person (employee) that is beneficial to the attacker and carries a false idea of voluntariness and independence of its acceptance by the object of influence. The social engineering techniques used are based on personality traits and their consideration in human decision-making. It is important to note that such methods are quite effective, simple and cheap to implement, and also have a low degree of risk. The article provides data characterizing the share of the impact of such methods on individuals and legal entities. In Russia, social engineering methods have become quite widespread, and their share has increased significantly due to the growth of remote payment transactions, the transfer of electronic documents and the increase in online services during the pandemic.

The main defense against social engineering, according to numerous claims by scientists and employers, is training. The study, during which a survey of students on information security issues was conducted, and it was also proposed to solve cases with information security breach situations through the use of social engineering technologies by an attacker, showed a low level of preparedness. There were no significant differences in the groups of students in different areas of training. Revealed the feasibility of adjusting programs.

Keywords: Information security, social engineering, training of students, methods of countering fraudsters, personal data, trade secrets, security threats.

References

1. Mitnick, Kevin David. The art of deception: controlling the human element of security / Kevin D. Mitnick & William L. Simon. – Indianapolis, Ind.: Wiley, cop. 2002.

2. Siadati, H. Mind your SMSes: Mitigating social engineering in second factor authentication / H. Siadati, T. Nguyen, P. Gupta, M. Jakobsson, N. Memon // Computers & Security. – 2017. – T. 65. – P. 14-28.

3. GOST R 50922-2006 Information security. Basic terms and definitions. URL: https://technical_translator_dictionary.academic.ru/239897/техническая_защита_информации (accessed: 1.02.2021)

4. GOST R 53114-2008: Information security. Ensuring information security in the organization. Basic terms and definitions. URL: http://docs.cntd.ru/document/1200075565 (date of request: 1.02.2021).

5. Information security in 2021. Threats, and industry trends. Company blog ITGLOBAL.COM. URL: https://habr.com/ru/company/itglobalcom/blog/540748/ (accessed: 5.02.2021).

6. Research. Current cyber threats in the second quarter of 2019. URL: https://ptsecurity.com (accessed: 7.02.2021)

7. Karpenko L. A., Petrovsky A.V., Yaroshevsky M. G. Kratkii psikhologicheskii slovar' [A Brief Psychological Dictionary]. Rostov-on-Don: "PHOENIX". 1998.

8. The number of attacks using social engineering increased by 147% in 2020. URL: https://www.securitylab.ru/news/515178.php: https://www.securitylab.ru/news/515178.php (accessed: 11.02.2021). In Rus.

9. A brief introduction to Social Engineering. URL: https://habr.com/ru/post/83415/ (accessed: 15.02.2021). In Rus.

10. Kuznetsov M.V.. Simdyanov I.V. *Sotsial'naya inzheneriya i sotsial'nye khakery* [Social engineering and social hackers.. St. Petersburg: BHV-Petersburg, 2007.

11. Review of TAdviser. Social engineering. URL: https://www.tadviser.ru/index.php (accessed: 05.02.2021). In Rus.

12. Review of reporting on information security incidents during the transfer of funds in the first and second quarters of 2019-2020. Bank of Russia. URL: https://yandexwebcache.net/yandbtm?lang=ru&fmode=inject&tm=1613241333&tld=ru&la=1612962048&text=статистика%20социальной%20инженерии%202020&url=https%3A%2F%2Fcbr.ru%2Fanalytics%2Fib%2Freview_1q_2q_2020%2F&l10n=ru&mime=html&sign=6e5cb27a99a583ff589c38b7aefc944c&keyno=0 (accessed: 11.02.2021). In Rus.

13. Ostanina E. A. Information security in the implementation of the BYOD concept. *Chelovecheskii kapital.* 2019. No. 12 (132). pp. 131-141. In Rus.

14. Ostanina E. A. About some aspects of facial recognition technology. *Chelovecheskii kapital.* 2020. No. 5 (137). pp. 142-152. In Rus.

15. Order of the Ministry of Education and Science of the Russian Federation of September 12, 2013 N 1061 "On Approval of Lists of specialties and areas of higher Education training" (with amendments and additions) Appendix N 1. List of areas of higher education – Bachelor's degree. URL: https://base.garant.ru/70480868/53f89421bbdaf741eb2d1ecc4ddb4c33/ (accessed: 12.02.2021).

16. Social engineering in Russia is more effective than in other countries. URL: https://habr.com/ru/news/t/459278/ (accessed: 15.02.2021). In Rus.

Ostanina Elena Anatolyevna. E-mail: neka1818@mail.ru