Научная статья
УДК 378+304
https://doi.org/10.24412/2658-638X-2025-4-237-240
EDN: https://elibrary.ru/aygvme
NIION: 2018-0077-4/25-696
MOSURED: 77/27-024-2025-04-895

Область науки: 5. Социальные и гуманитарные науки
Группа научных специальностей: 5.8. Педагогика
Шифр научной специальности: 5.8.1. Общая педагогика, история педагогики и образования

Человек как основной источник распространения конфиденциальной информации

Елена Петровна Челак
Московский университет МВД России имени В.Я. Кикотя, Москва, Россия, Motyscheva.elena@yandex.ru

Аннотация. Проводится исследование влияния «человеческого фактора» на безопасность информации.
Ключевые слова: защита информации, человеческий фактор, конфиденциальная информация, социальная инженерия, перечень документов
Для цитирования: Челак Е. П. Человек как основной источник распространения конфиденциальной информации // Психология и педагогика служебной деятельности. 2025. № 4. С. 237–240. https://doi.org/10.24412/2658-638X-2025-4-237-240. EDN: AYGVME.

Original article

Man as the main source of confidential information distribution

Elena P. Chelak
Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot', Moscow, Russia,
Motyscheva.elena@yandex.ru

Abstract. A study is being conducted to examine the impact of the «human factor» on information security.
Keywords: information protection, human factor, confidential information, social engineering, list of documents
For citation: Chelak E. P. Man as the main source of confidential information distribution // Psychology and pedagogy of service activity. 2025;(4):237–240. (In Russ.). https://doi.org/10.24412/2658-638X-2025-4-237-240. EDN: AYGVME.

В наше время, в условиях развивающихся технических возможностей, информация приобретает особую значимость и является целью добычи посторонними лицами. Технологии по защите информации не стоят на месте, с каждым годом внедряются новые совершенные методы защиты информации. Компании пытаются защитить свою конфиденциальную информацию техническими методами, в то же время опуская, либо недооценивая человеческий фактор.

Если рассматривать информацию как средство обогащения либо средство власти, то в мире всегда есть две стороны, одни мечтают продать информацию, другие ее получить. Кроме этого, существуют еще один способ утечки информации – халатность либо недобросовестность оператора. Также значительный фактор риска, который часто остается в тени, – человеческие ошибки.

На сайте информационного портала газеты «Известия» в статье «В чем главные причины ИБ-инцидентов в России» приведены сведения, что, по данным центра противодействия киберугрозам Innostage SOC CyberART, за первое полугодие 2024 года 80 % всех утечек данных происходят по вине сотрудников [1]. Представьте себе, что даже одна ошибка, например, неправильно введенный пароль или неверный клик, может обойти современные системы безопасности. Самая мощная защита бессильна, если сотрудники компании допускают ошибки: отправляют файлы не по тому адресу, сохраняют пароли в небезопасных местах или кликают на фишинговые ссылки. Это делает доступ к корпоративным данным для хакеров проще, чем через любые программные уязвимости.

Злоумышленники, владея типовой поведенческой психологией людей, эксплуатируют человеческие слабости, такие как доверчивость, любопытство, страх, желание оказать помощь или произвести впечатление для доступа к ограниченной информации, например к паролям доступа к различным защищенным информационным ресурсам как самих людей, так и организаций, в которых эти люди работают. Данный вид мошенничества получил название – социальная инженерия.

«Социальные» мошенники постоянно совершенствуют методы и способы неправомерного доступа к ценной информации.

Методы социальной инженерии можно квалифицировать по различным критериям.

По способу взаимодействия с жертвой выделяют прямые и косвенные методы.

Прямые методы предполагают непосредственный контакт между злоумышленниками и жертвой. К ним относятся личные встречи, телефонные звонки, видеоконференции и другие способы прямого общения. Преимуществом данного подхода для правонарушителей является адаптация стратегии воздействия в реальном времени на основе реакции жертвы.

Косвенные методы не требуют прямого взаимодействия и могут реализовываться через электронную почту, SMS-сообщения, публикации в социальных сетях, размещение вредоносных файлов на каких-либо устройствах, которые могут заинтересовать жертву. Такие методы позволяют злоумышленникам оставаться анонимными и охватывать большое количество потенциальных жертв одновременно.

По степени персонализации атак различают массовые и целенаправленные.

Массовые атаки нацелены на широкую аудиторию без детального изучения конкретной потенциальной жертвы.

Целенаправленные атаки предполагают тщательное изучение конкретной жертвы или организации. Злоумышленники собирают детальную информацию о структуре компании, ее сотрудниках, используемых технологиях и бизнес-процессах для создания максимально убедительных сценариев «социального» воздействия.

Эффективность социальной инженерии основывается на глубоком понимании психологических механизмов принятия решений и человеческого поведения. Выделяет следующие принципы [2], которые активно используются в социально-инженерных атаках:

– принцип взаимности основан на естественном стремлении людей отвечать добром на добро. Злоумышленники могут предложить небольшую услугу или подарок, создавая ощущение долга у жертвы;

– принцип последовательности эксплуатирует желание людей действовать в соответствии со своими предыдущими заявлениями или поступками. Получив согласие на небольшую просьбу, злоумышленник может постепенно увеличивать требования;

– принцип социального доказательства использует склонность людей ориентироваться на поведение других в неопределенных ситуациях. Ссылки на то, что «все так делают» или «другие сотрудники уже предоставили такую информацию», могут снизить бдительность жертвы;

– принцип симпатии основан на том, что люди более склонны соглашаться с теми, кто им нравится. Злоумышленники могут использовать общие интересы, комплименты или схожие взгляды для установления доверительных отношений;

– принцип авторитета эксплуатирует готовность людей подчиняться тем, кого они воспринимают как авторитетных фигур. Выдавая себя за руководителя, IT-специалиста или представителя службы безопасности, злоумышленники могут добиться выполнения своих требований;

– принцип дефицита использует страх упустить ограниченную возможность. Создание искусственного чувства срочности заставляет жертв действовать быстро, не успевая критически оценивать ситуацию. Развитие информационных технологий существенно увеличило возможности «социальных инженеров» и изменило характер их деятельности. В доцифровую эпоху социальная инженерия ограничивалась преимущественно личными контактами и телефонными звонками. Злоумышленники полагались на базовые навыки убеждения и ограниченную информацию, которую можно было получить из открытых источников.

С появлением Интернета и социальных сетей ситуация кардинально изменилась. Современные «социальные инженеры» получили доступ к огромным объемам персональной информации, размещаемой пользователями добровольно. Анализ профилей в социальных сетях позволяет создавать детальные психологические портреты потенциальных жертв, изучать их интересы, связи, места работы и личные предпочтения.

Социальная инженерия сейчас представляет собой фундаментальную угрозу информационной безопасности, которая эволюционирует вместе с развитием технологий и изменением социальных практик. Без понимания ее природы и методов реализации невозможно организовать эффективную защиту информации.

Организации тратят огромные суммы на защиту данных техническими способами, но без обучения собственного персонала и проведения профилактической работы с сотрудниками все усилия могут оказаться напрасными.

Рассмотрим часто встречающиеся проблемы защиты информации, неправильные действия, совершаемые сотрудниками при обработке информации ограниченного пользования: распространенными ошибками являются такие, как обработка информации конфиденциального характера на ПЭВМ, не предназначенных для данной работы, а также отправка конфиденциальных данных по неверному адресу, данные ошибки могут иметь фатальные последствия. Кроме этого, можно обнаружить в свободном доступе пароли сотрудников, прикрепленные на ПЭВМ. Либо оставленные без контроля, включенными компьютеры, на которых обрабатывается конфиденциальная информация. Периодически сотрудники технической защиты информации обнаруживают выходы со служебных компьютеров в Интернет на онлайн-платформы, используемые для общения, это подтверждает факты использования компьютеров, на которых обрабатываются персональные данные, в личных целях. Все эти факты свидетельствуют о возможности свободного доступа к данным третьих лиц, т. е. утечки конфиденциальной информации.

Злоумышленники часто используют психологические уловки, чтобы добыть ценную информацию у сотрудников. Для этого не нужно сложное оборудование, достаточно просто обмануть человека, например маскируются электронные письма под доверенные источники – от клиентов, поставщиков или даже руководства компании. У специалистов по технической защите информации данный способ добычи злоумышленниками информации получил название фишинг (от английского слова «fishing», что означает рыбалка). Ничего не подозревающий сотрудник открывает письмо и выполняет предложенные действия, тем самым дает преступникам доступ к системам компании.

С развитием систем искусственного интеллекта методы воздействия на персонал организации становятся все более изощренными. Так, например, злоумышленники освоили синтез голоса конкретного человека. Буквально с недавнего времени некоторым сотрудникам стали поступать телефонные звонки от якобы начальства голосами очень похожими на настоящих руководителей организации. «Лжеруководители» по телефону пытаются убедить подчиненных выполнить какие-либо действия, исполнение которых может нанести вред организации.

Еще одним из способов причинения вреда организации при помощи человеческого фактора является размещение (бесплатная раздача) каких-либо технических устройств, например, USB-накопителей с размещенными на них вредоносными программами. Любопытство или желание помочь часто приводят к подключению таких устройств к корпоративным компьютерам, что может привести к компрометации системы.

Именно поэтому человеческий фактор остается самым слабым звеном в системе безопасности компании. Недооценка этого аспекта может привести не только к финансовым потерям, но и к дискредитации компании. Вкладывая финансовые ресурсы в большом объеме в техническую защиту информации, организация всегда будет оставаться под ударом хакеров, если не будет проводиться работа с сотрудниками компании.

Одна из мер по предотвращению утечки информации от человека начинается с первых шагов трудоустройства потенциальных сотрудников, это – профилактическая беседа сотрудников технической защиты информации с кандидатами на должность, разъяснение норм и правил работы с конфиденциальной информацией. Закрепление в должностном регламенте сотрудника ответственности за неправомерные деяния, приводящие к утечке информации, подписание им документов о соблюдении требований по работе с конфиденциальной информацией. Каждый кандидат на должность должен осознавать важность информационной безопасности и нести ответственность за разглашение информации конфиденциального характера.

Для избежания двойственной трактовки понятия «конфиденциальная информация» в организации должен быть разработан и нормативно утвержден перечень документов, подпадающих под конфиденциальную информацию, информацию для служебного пользования, персональные данные.

Разработка методических рекомендаций, понятных для пользователей, обучение сотрудников компании с регулярным проведением тренингов по защите информации с учетом современных механизмов противодействия атакам социальной инженерии способствует уменьшению рисков по утечки информации от человека. Чем компетентней сотрудники организации, тем меньше шансов у хакеров на успешную атаку.

Создание эффективной культуры безопасности требует времени и последовательных усилий со стороны руководства организации. Однако инвестиции в развитие человеческих ресурсов безопасности часто оказываются более эффективными, чем вложения в технические решения, особенно в контексте защиты от социально-инженерных атак, которые по своей природе направлены на эксплуатацию человеческого фактора.

Библиографический список

1. Известия 02.02.2025 // URL:// https://iz.ru/newspaper/no19-2-fevralia-2025-goda.

2. URL://https://trinity-mission.ortox.ru/files/2016/03/Chaldini-Psihologiya-vliyaniya.pdf.

Bibliographic list

1. Izvestia 02.02.2025 // URL://https://iz.ru/ newspaper/no19-2-fevralia-2025-goda.

2. URL://https://trinity-mission.ortox.ru/files/2016/03/Chaldini-Psihologiya-vliyaniya.pdf.

Информация об авторе

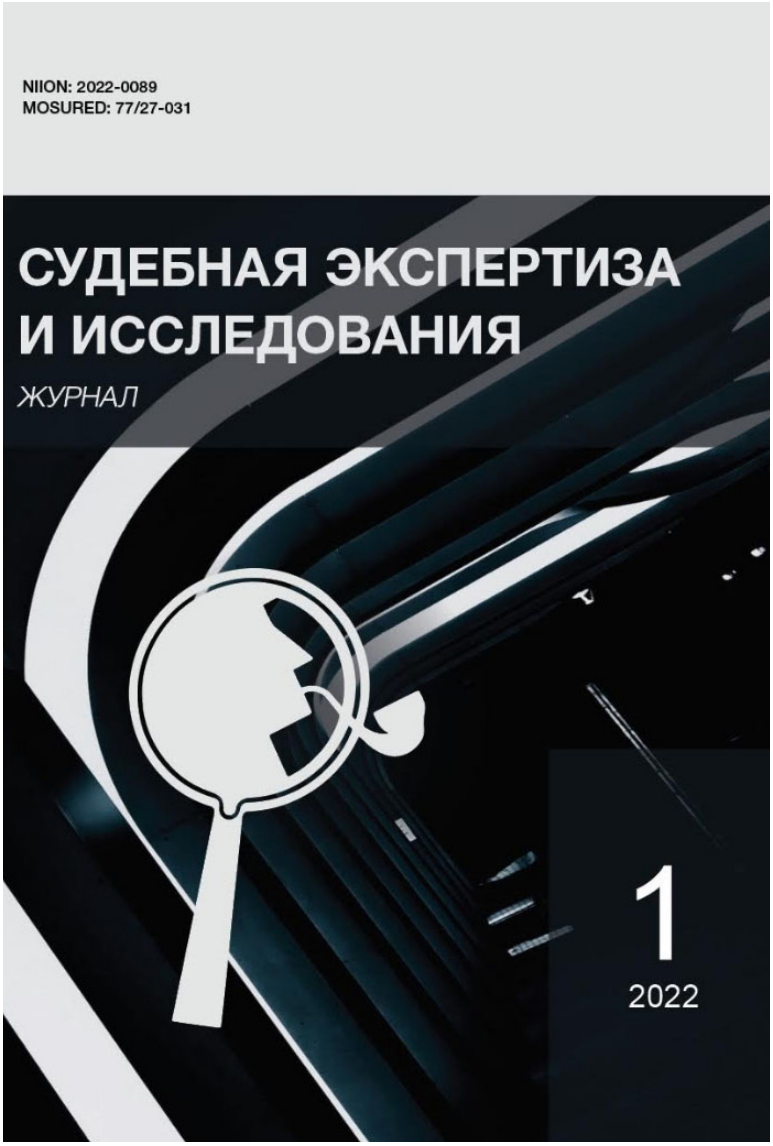
Е. П. Челак – старший преподаватель кафедры специальных информационных технологий учебно-научного комплекса информационных технологий Московского университета МВД России имени В.Я. Кикотя.

Information about the author

E. P. Chelak – Senior lecturer of the Department of Special Information Technologies of the Educational and Scientific Complex of Information Technologies of the Moscow University of the Ministry of Internal Affairs of Russia named after V.Ya. Kikot'.

Статья поступила в редакцию 02.07.2025; одобрена после рецензирования 28.11.2025; принята к публикации 01.12.2025.

The article was submitted 02.07.2025; approved after reviewing 28.11.2025; accepted for publication 01.12.2025.



Журнал ***«Судебная экспертиза и исследования»*** *приглашает к сотрудничеству аспирантов, докторантов и соискателей, а также всех заинтересованных лиц.*

Главный редактор журнала: заслуженный деятель науки Российской Федерации, заслуженный юрист Российской Федерации, почетный профессор Университета правоохранительной службы Монголии, почетный член Литовского криминалистического общества, член Международного сообщества судебных экспертов, доктор юридических наук, профессор Надежда Павловна Майлис.

Журнал расширяет платформу для дискуссий ученых и практиков по насущным вопросам назначения, организации, проведения всех видов судебных экспертиз, а также производства исследований, в том числе с применением инновационных технологий.

Адрес редакции:123298, г. Москва, ул. Ирины Левченко, д. 1.

E-mail: sud-ekspertiz@mail.ru

Телефон: +7 499 740-68-30