ПЕРСПЕКТИВНЫЕ И НЕСТАНДАРТНЫЕ НАПРАВЛЕНИЯ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Выполнил студент бакалавриата,
техник по защите информации:
Емельянов Григорий Андреевич

Москва, 2024

Перспективные и нестандартные направления в области информационной безопасности

Аннотация. *Статья посвящена лишь некоторым перспективным и нестандартным направлениям, которые предстоит исследовать специалистам и научному сообществу в будущем. Полученные результаты и материалы могут быть использованы для совершенствования научной и методической базы исследований в области информационной безопасности и других технических направлений.*

Выявление новых скрытых каналов передачи информации

Выявление новых скрытых каналов (стеганографических методов) крайне необходимо для сохранения большей конфиденциальности передачи информации. Осуществлять передачу информации возможно не только используя текст, содержащий машинописный или рукописный ввод. Например, передавать информацию можно с помощью электромагнитных и электрических импульсов, радиоволн, света и других искусственно созданных физических свойств, или с помощью мимики и жестов, заранее обговоренного поведения (действий) и их значений. При передаче информации важно сохранить её целостность, доступность и конфиденциальность. Для обеспечения конфиденциальности передаваемой информации необходимо действовать нестандартно, создавая злоумышленнику трудности, например маскировать передачу разными способами. В 2023–2024 годах было выявлено 2 новых скрытых канала передачи информации:

- Модулирование жидкостного потока. Передача информации таким способом осуществляется посредством модулирования жидкостного потока (например воды), что позволяет передавать сигналы на небольшие расстояния (1–10 метров). Скрытый способ передачи информации, при помощи транспортировки жидкости, будет иметь одно главное преимущество перед стандартными каналами связи, а именно незнание злоумышленника о том, что информация передаётся таким образом, исключая какую-либо возможность

перехвата данных. Такой способ в классификации стеганографии занимает место материально-физических методов.

- Вызов цепочки мыслей ассоциативного ряда. Если у человека можно вызывать определённые мысли с помощью каких-то действий (например, отправить картинку, видео, текст, пообщаться, посмотреть вместе фильм, позвать на ужин и т. д.), то их можно и частично считывать (т. е. истинно предполагать о чём думает человек). В мозгу возбуждение множества нейронов вызывает и лёгкое возбуждение соседних нейронов, которые будут как бы "издалека" приводить к другим размышлениям. Например, при просмотре фильма у двух людей будут возникать примерно одни и те же эмоции, которые влекут за собой рассуждения и мысли, в том числе и схожие. Т. е. вызывая у человека какую-то мысль, она повлечёт за собой цепочку ассоциативного ряда, где одна мысль из ряда будет скрытым посланием. Такой способ в классификации стеганографии занимает место нестандартных методов.

Таким образом, выявление новых скрытых каналов передачи информации является одной из самых важных тем сохранения конфиденциальности информации. При этом скрытые каналы на данный момент не пользуются большой популярностью ни среди специалистов, ни среди научного сообщества, по сравнению с другими направлениями.

Скрытое обеспечение информационной безопасности

На данный момент методы скрытого обеспечения информационной безопасности довольно мало используются. Предприятия в открытом доступе объявляют о своих мерах безопасности для привлечения клиентов и повышения репутационного статуса, и это достаточно оправдано, поскольку потребителей интересуют вопросы безопасности и конфиденциальности информации в используемых сервисах и системах. С другой стороны, такое поведение предприятий даёт простор злоумышленникам для проведения разного рода атак, т. к. они легко узнают методы и средства безопасности,

используемые технологии в компании. Далее описывается несколько примеров того, как можно скрытно обеспечивать информационную безопасность в компании, а также сохранять в тайне меры безопасности на предприятии, при этом не вызывая подозрений и не теряя репутационного статуса.

Предположим, что конфиденциальное помещение в компании обеспечено железной дверью на входе для защиты от физического доступа к секретным документам. Тогда злоумышленник знает, что данное помещение является значимым для компании. Можно ввести в заблуждение злоумышленника, установив железную дверь в какой-нибудь подсобный кабинет. Можно везде устанавливать защищённые железные двери. Но наилучшим решением будет поставить железную дверь у входа в конфиденциальное помещение и оббить её деревянным каркасом. В этом случае свою роль играет как раз скрытое обеспечение информационной безопасности. Помещение не вызывает подозрений и при этом оно хорошо защищено от проникновения.

Вместо того, чтобы рассказывать какие методы и средства обеспечения информационной безопасности используют на предприятии, уместнее было бы легендировать такие разговоры, а не давать злоумышленникам лишней информации. Используя технологию шифрования А, мы будем говорить, что используем технологию Б, равную ей по уровню защищённости. Таким образом исключим возможность атаки на сеть и системы, учитывая то, что у злоумышленников ложная информация. Для потребителей можно использовать такую формулировку: "Мы настолько ответственно подходим к обеспечению информационной безопасности нашей компании, что не будем говорить какие средства и технологии используем, а также умолчим если вы хотите знать наши аутентификационные данные".

Это лишь несколько довольно абстрактных примеров, но они точно описывают суть данных мер. Такие меры можно применять и к другим видам деятельности компании. Подобный уровень закрытости может оттолкнуть потенциальных клиентов, но может и привлечь, если объяснение мер

безопасности будут выдавать потребителям по необходимости в виде соответствующих от них запросов или при личной встрече.

«Безопасность через неясность» («security through obscurity»)

Система, полагающаяся на «безопасность через неясность», может иметь существующие или предполагаемые уязвимости, но её владельцы или разработчики считают, что если недостатки неизвестны, то злоумышленник не сможет их обнаружить. Система может также использовать безопасность через неясность в качестве одного из уровней защиты системы, поскольку даёт время разработчикам системы устранить найденную уязвимость, тогда как публичное раскрытие продуктов и версий делает их основной целью для использования обнаруженных уязвимостей в этих продуктах и версиях. Первым шагом злоумышленника обычно является сбор информации: эта задача усложняется при использовании безопасности через неясность.

Следует отметить, что вопреки общему мнению, данный подход не подразумевает отсутствие аудита или тестирования на защищённость. Он подразумевает лишь то, что итоги проведённого аудита будут известны ограниченному кругу лиц.

Вариант базового принципа «безопасности посредством меньшинства» основан на характеристиках малоизвестных программ, при использовании которых снижается вероятность обнаружения уязвимостей в случайных и автоматических атаках. Этот подход имеет множество названий, и является очень распространённым. Также существуют термины «безопасность посредством редкости», «безопасность посредством непопулярности», «безопасность по причине отсутствия интереса». Например, программные продукты или системы, используемые компанией, могут быть написаны на мало известных или устаревших языках программирования таких как R, D, Kotlin, Pascal, Lua, Perl и др., исключая возможность быстрого и лёгкого анализа программ злоумышленникам. К этому же подходу относится и

обфускация программного кода, и использование закрытого (или мало известного) программного обеспечения.

У данного подхода есть много плюсов и минусов, например, при использовании принципа «безопасность через неясность» безопасность может быть нарушена не только злоумышленником, но даже и случайным человеком. Однако иногда такие меры бывают вынужденными и частичное необходимое их соблюдение может помочь в сохранении обеспечения информационной безопасности.

Кадровая безопасность через контроль

Для упрощения работы в компании, в том числе при работе с конфиденциальной информацией необходимо быть уверенным в своих сотрудниках. Кадровая защита информации может походить на организационную и, возможно, является одной из её множества больших разделов постепенно уходя в самостоятельную часть. К основным группам качеств для сравнения кандидатов относятся: профессиональные, образовательные, организационные и личные. Основным требованием при отборе является тщательное изучение деловых, моральных и этических данных каждого, в частности особое внимание уделяется специалистам по защите информации.

В некоторых ситуациях специалист по информационной безопасности может проговориться или выдать конфиденциальную информацию, секреты и тайны компании, например:

- Социальные сети. Фотографии и видео с места работы могут дать пищу для размышлений злоумышленникам, особенно метаданные или местоположение сделанного снимка. Даже в случае закрытого аккаунта специалиста, злоумышленник (в частности, социальный инженер) может напроситься к нему в подписчики или друзья, втереться в доверие, представившись одинокой красивой девушкой или человеком, со схожими взглядами/интересами.

- Гаджеты и рабочее место специалиста. Оставленный гаджет, ноутбук, ПК, без присмотра, без блокировки и пароля, предоставит возможность другому сотруднику получить критически значимую информацию, внедрить своё вредоносное ПО или скомпрометировать (подделать, сымитировать) действия от его имени. Рабочее место также может дать много интересной информации, но это скорее относится к косвенным признакам.
- Непринуждённый разговор. Общение специалиста по ИБ о деятельности работы с сотрудниками, не имеющими соответствующего доступа к значимой информации, приведёт к тому, что этот сотрудник получит информацию, которую знать не должен. Затем он может использовать эту же информацию для продажи злоумышленникам. Также во время беседы специалист может говорить слишком громко или в присутствии большого количества людей о своей деятельности, что повлечёт утечку критической информации.
- Недостаточная осведомленность о конфиденциальности и секретах.
- Слабая компетентность при выполнении своей работы.
- Косвенные признаки. Настроение специалистов подразделения ИБ, их поведение, время прихода/ухода с работы, загруженность, внешний вид, частые вызовы к руководству и др. Все эти признаки могут послужить для дальнейшего анализа.
- Психологическое или физическое воздействие на специалиста. Под психологическим воздействием понимаем угрозы, запугивание, шантаж, давление на семью и родственников, обман (и введение в заблуждение), подставные методы, гипноз и т. п. Физическое воздействие — это причинение вреда здоровью, пытки, избиение, издевательства, надругательство, гипноз, введение «Сыворотки правды» и т. п. «Сыворотка правды» — условное название психоактивных веществ, используемых (чаще всего спецслужбами) для получения скрываемых человеком сведений. Законность (а также

эффективность) таких методов вызывает сомнение. Некоторые считают, что их можно рассматривать как пытку или, по крайней мере, как жестокое и бесчеловечное обращение, запрещённое международным правом. Такие методы применяются в основном против военных офицеров, специалистов спецслужб, агентов и разведчиков, важных руководителей крупных корпораций, олигархов, террористов и главарей ОПГ, серийных убийц, и людей, находящихся определённого вида власти государства.

Обладая большим количеством секретной информации и доступом к ней, специалистам по защите информации важно быть осторожными в своих действиях. Поскольку сотрудники отдела информационной безопасности работают с государственными и коммерческими тайнами, с другими видами секретов и в целом знают больше остальных об организации сетевой инфраструктуры, уязвимостях и слабых местах, организационном управлении и т. д., то, как правило, в больших корпорациях их контролируют отдельные секретные разведывательные отделы, которые не известны никому, кроме генерального директора или собственника предприятия.

Данные сотрудники, как правило, не трудоустроены официально (или устроены на другие должности) и посещают предприятие в исключительных случаях. Их цель отслеживать действия специалистов по ИБ и незаметно их контролировать разными видами слежки. Речь идёт об установлении особого контроля, как технического, так и физического, улавливание психологического состояния, настроения, изменения в поведении специалистов. Сотрудникам разведывательного отдела должен доверять генеральный директор, при этом их не должно быть слишком много, как правило, это несколько человек.

Иерархия контроля в общем виде может выглядеть следующим образом: генеральный директор – разведывательный отдел – отдел информационной безопасности – остальные сотрудники компании (рис. 1). У каждого из данной иерархии свой уровень доступа в компанию и навыки контроля за остальными. Это означает, что разведывательный отдел скорее всего не будет следить за всеми сотрудниками компании, так как не имеет для этого подходящего статуса

и места в компании. При этом генеральный директор может взаимодействовать со всеми. Сотрудники отдела информационной безопасности имеют наибольший простор для контроля и отслеживания всех сотрудников и бизнес-процессов компании.

Рисунок 1 – Иерархия контроля в компании

Таким образом, используя данную организацию иерархии можно построить качественную систему информационной безопасности, где специалисты по ИБ будут находиться под соответствующим контролем, сами того не подозревая. Обычно, в формировании в коллективе дополнительных этических норм заинтересован и сам персонал. К подобным средствам относится формирование особой корпоративной культуры.

Информационные атаки

В последнее время специалисты по расследованию высоко технологичных киберпреступлений стали также заниматься разбором информационных атак в связи с соответствующей потребностью клиентов. Информационные атаки стали популярным методом, который довольно легко реализуется, поэтому в будущем специалисты по информационной безопасности должны будут заботиться не только о технических аспектах, но и о социальных, в том числе отслеживание репутации и статуса компании.

Информационные атаки и дезинформация стали неотъемлемой частью современной реальности. Развитие технологий, доступность информации и распространение социальных сетей создают благоприятную среду для манипулирования общественным мнением, дискредитации и подрыва доверия.

Современные информационные атаки используют широкий спектр методов, от распространения ложной информации и пропаганды до кибератак и дискредитации личности. Особую опасность представляет дезинформация, которая использует психологические и социальные факторы для формирования искаженного восприятия реальности.

На рисунке 2 представлена общая схема дезинформации. Ложь 1 — это настоящая ложь, а Ложь 2 — ложь, которую представляют в виде истины (в том числе, приводя в аргумент очевидную Ложь 1). Истину могут видеть те, кто знает о ней и понимает эту схему управления.

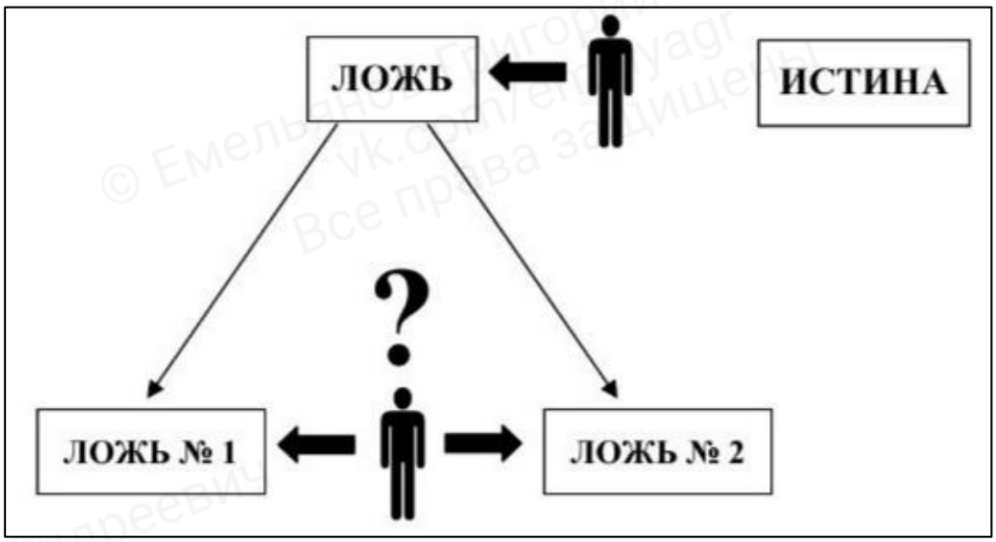

Рисунок 2 – Схема дезинформации

В век информатизации дезинформация играет важнейшую роль. Предположим, субъект А обвиняет субъект Б. Субъект Б обвиняет субъект А в ложных обвинениях. В свою очередь Б обвиняет А, преподнося полностью противоположную информацию. Возникает большой и спорный вопрос доверия субъектам среди следящих за ситуацией. Как правило, доверие будет основано не столько на объективных факторах, сколько на субъективных, которые могут быть вызваны когнитивными искажениями. В таком случае необходимо стараться стремиться к объективизму через призму небольшого скептицизма и сомнения: полностью доверять нельзя никому, если человек не видел это вживую своими глазами. Нужно анализировать все виды источников разных систем и мнений. Ошибочно будет смотреть, читать, слушать и

анализировать только одно системные источники информации. Они не дают понять настоящую картину происходящего, т. к. трактуют всё в свою пользу. Существует мнение, что дошедшую до человека информацию надо делить на 2, а то и на 3, 4, 5. Проходя путь от первоисточника, она могла быть модифицирована много раз, преувеличена или же наоборот, преподнесена в другой форме или с другим посылом. Далее будут представлены некоторые из подобных примеров дезинформации.

Перенос видео или аудио интервью в текстовый формат может сильно искажать действительность сказанного человеком. В видео интервью человек отвечает на вопросы не только словами, но и мимикой, жестами, тембром голоса, скрытыми посланиями, внешним видом и др. А в текстовом формате есть только слова. Если человек сказал что-то с ухмылкой, в шутку, или выражает своё же недопонимание ситуации, то такие неоднозначности будут перенесены в текст, как однозначные высказывания. Из-за этого смысл и восприятие сказанного, в виде текста, может полностью отличаться от того, что имел в виду человек. Точно так же и с перепиской. В сообщении человек не всегда может наиболее точно передать свои эмоции, мимику, жесты и т. п., но, хорошо зная собеседника в жизни можно предположить какие эмоции и мысли он хочет передать через данное сообщение, написав всего пару слов, без смайлов.

Важно понимать, что одна и та же информация (абсолютно идентичная), из разных источников, может трактоваться, восприниматься и, в связи с этим, оцениваться неоднозначно, учитывая контекст, её представление, вид источника и другие факторы. Далее будут представлены некоторые подобные примеры.

Пример восприятия от вида источника:

Телеканал Матч ТВ: «Сборная России по футболу обыграла сборную Сан-Марино со счётом 9–0» (информация воспринята однозначно).

Юмористическая телепередача Comedy Club: «Сборная России по футболу обыграла сборную Сан-Марино со счётом 9–0» (информация воспринята как шутка).

Пример вырывания информации из контекста.

[Первоисточник] «Журнал университета»: «70% студентов больше всего ценят в преподавателях лояльность, 20% – умение донести материал, 5% – организованность и 5% – компетентность».

[Недобросовестный источник] «Новостной вестник»: «5% студентов ценят в преподавателях компетентность». – «Журнал университета».

Таким образом, ссылаясь в конце на первоисточник, они снимают с себя ответственность за преподнесение информации в другом контексте. Примеры могут быть намного противоположнее и с более серьёзными последствиями.

Для защиты от информационных атак необходимо развивать критическое мышление, проверять информацию из разных источников, использовать проверенные информационные ресурсы и быть осторожными в отношении информации как из официальных, так и из неофициальных источников.

Полученные результаты и материалы статьи могут быть использованы для совершенствования научной и методической базы исследований в области информационной безопасности и других технических направлений