ствует какого-то одного универсального метода и методики оценки стоимости нематериальных активов.На наш взгляд, одной из наиболее приемлемых с точки зрения экономической практики методов оценки общей величины интеллектуального капитала является компонентно-инвестиционный метод, основанный на суммарной оценке всех видов (компонентов) осуществленных и накопленных инвестиций в интеллектуальный капитал с учетом различного периода инвестиционных вложений по видам вложений, а также продолжительности трудовой деятельности работника.

Необходимо совершенствовать методологию оценки уровня развития информационной экономики в странах, а также методологию оценки **интеллектуального капитала, являющегося сегодня главным фактором инновационного экономического роста.**

Список использованных источников:

1.Иноземцев В.Л. За пределами экономического общества. Постиндустриальные теории и постэкономические тенденции в современном мире. Электронная версия. http://www.inozetmtsev.net

2.Доклад Организации Объединенных Наций об информационной экономике 2007/2008 год «Наука и техника на службе развития: Новая парадигма ИКТ». Нью-Йорк - Женева, 2007. С. 33.

3. Д. Белл. Грядущее постиндустриальное общество. — М.: Академия, 1999.

4.Дятлов С.А. Интеллектуально-информационный капитал / Государство и рынок: новое качество взаимодействия в информационно-сетевой экономике / Под. ред. проф. С.А. Дятлова, проф. Д.Ю. Миропольского, проф. В.А. Плотникова. Т. 1. СПб.: Астерион, 2007. С. 280-289.

5. Дятлов С.А., Марьяненко В.П., Селищева Т.А. Информационно сетевая экономика: структура, динамика, регулирование. СПб., 2008.

6. А. Глинчикова. Россия и информационное общество. — М.: АСТ, 2002. с.32.

7. В. Шульцева. Мировой цифровой ринг: тенденции, метаморфозы, цифры, прогнозы. IT-News №1, IT-Weekly №4, 2013.

8. Лемещенко П.С., Шумских Е.В. Информационная экономика Республики Беларусь в контексте мировых тенденций развития. Минск. Мисанта. 2013

9 .Global Competitive Report 2001-2004, World Economic Forum, 2004.

10. Наука и инновационная деятельность в Республике Беларусь: стат. сб. [Электронный ресурс]. — Режим доступа: www.scienceportal.org.by/reports/aa44328e63d1a71c.html. Nauka i innovatsionnaya deyatel'nost' v Respublike Belarus': stat. sb. [Electronic resource]. — Mode of access: www. scienceportal.org.by/reports/aa44328e63d1a71c.html.

11. http://www.comnews.ru: http://http://www.comnews.ru

СОЦИАЛЬНЫЙ ИНЖИНИРИНГ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Жишкевич Д.В., Литвинко О.В.

Власова Г.А. – канд. экон. наук., доц.

Целью работы является изучение основных принципов социальной инженерии. Предметом является рассмотрение основных методов социальной инженерии - по мнению многих исследователей одного из основных инструментов хакеров XXI века.

Многие исследователи считают, что социальная инженерия станет одним из основных инструментов хакеров XXI века, потому что технические системы защиты будут все больше и больше совершенствоваться, а люди так и будут оставаться людьми со своими слабостями, предрассудками, стереотипами, и будут самым слабым звеном в цепочке безопасности. Задача хакера состоит в том, чтобы взломать компьютерную систему. Поскольку, как мы видим, у этой системы две составляющие, то и основных путей ее взлома соответственно два. Первый путь, когда "взламывается компьютер", мы назовем техническим. А *социальной инженерией* называется то, когда, взламывая компьютерную систему, вы идете по второму пути и атакуете человека, который работает с компьютером. Таким образом, социальная инженерия — это метод управления действиями человека без использования технических средств. Метод основан на использовании слабостей человеческого фактора и считается очень разрушительным. Сегодня социальную инженерию зачастую используют в интернете для получения закрытой информации, или информации, которая представляет большую ценность.

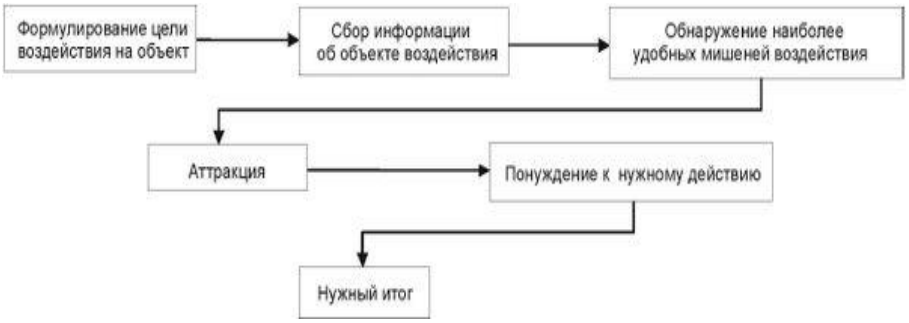

Рис. 1 Основная схема воздействия в социальной инженерии

Итак, сначала всегда формулируется цель воздействия на тот или иной объект. Затем собирается информация об объекте, с целью обнаружения наиболее удобных *мишеней воздействия*. После этого наступает этап, который психологи называют *аттракцией*. Аттракция - это создание нужных условий для воздействия социоинженера на объект. Принуждение к нужному для социального хакера действию обычно достигается выполнением предыдущих этапов, т. е. после того, как достигнута аттракция, жертва сама делает нужные социоинженеру действия. Однако в ряде случаев этот этап приобретает самостоятельную значимость, к примеру, тогда, когда принуждение к действию выполняется путем введения в транс, психологического давления и т. д.

Для проведения своих атак злоумышленники, применяющие техники социальной инженерии, зачастую эксплуатируют доверчивость, лень, любезность и даже энтузиазм пользователей и сотрудников организаций. Защититься от таких атак непросто, поскольку их жертвы могут не подозревать, что их обманули. Злоумышленники, использующие методы социальной инженерии, преследуют, в общем, такие же цели, что и любые другие злоумышленники: им нужны деньги, информация или ИТ-ресурсы компании-жертвы. Для защиты от таких атак нужно изучить их разновидности, понять, что нужно злоумышленнику, и оценить ущерб, который может быть причинен организации.

Методы решения внутренних угроз:

Очень часто, когда речь заходит о безопасности предприятия, в том числе, когда дело касается социальной инженерии, предприятия защищаются только от внешней угрозы, совершенно забывая о том, что опасность может быть внутри.

Наблюдение за сотрудниками на всех стадиях их развития в организации. При приеме сотрудника на работу необходимо собрать о нем как можно больше сведений, с целью прогноза того, как он поведет себя в той или иной ситуации. Основная проблема состоит в том, что за сотрудником, если и наблюдают, то только в период его устройства на работу. В лучшем случае - в период его работы на предприятии. И практически никто не проводит работу с увольняющимися сотрудниками, хотя они и представляют основную угрозу для безопасности предприятия.

Если сотрудники лояльно относятся к своему предприятию и руководству, то большинство атак социальных хакеров пройдет мимо этого предприятия. Это значит, что человек доволен работой на предприятии, как в моральном, так и в материальном плане. Кроме того, лояльность сотрудников зависит еще и от того, какой способ управления принят на предприятии.

Незаменимых сотрудников нет. многие сотрудники, почувствовав свою значимость, начинают нередко попросту шантажировать руководителя.

Необходимы реальные инструктажи, на предмет того, каким атакам может подвергнуться предприятие, и что конкретно взятый сотрудник может сделать на своем месте, чтобы этой атаки не произошло. Проведение инструктажей является обязательным. Дело в том, что человек может просто не знать, что та или иная проблема существует. А если и знает, то решит ее, в случае возникновения, гораздо быстрее, если будет четкий алгоритм решения проблемы. Потому что когда проблема возникает, то нужно ее решать, а не изобретать способы ее решения. Это желательно сделать заранее.

Внешние угрозы:

Угрозы, связанные с электронной почтой. Большинство мер по обеспечению безопасности направлены на предотвращение доступа неавторизованных пользователей к корпоративным ресурсам. Если, щелкнув присланную злоумышленником гиперссылку, пользователь загрузит в корпоративную сеть троянскую программу или вирус, это позволит легко обойти многие виды защиты. Гиперссылка может также указывать на узел с всплывающими приложениями, запрашивающими данные или предлагающими помощь. Как и в случае с другими разновидностями мошенничества, самым эффективным способом защиты от атак злоумышленников является скептическое отношение к любым неожиданным входящим письмам. Для распространения этого подхода в организации в политику безопасности следует включить конкретные принципы использования электронной почты, охватывающие следующие элементы:Вложения в документы, гиперссылки в документах, запросы личной или корпоративной информации, исходящие изнутри компании, запросы личной или корпоративной информации, исходящие из-за пределов компании.

Угрозы, связанные с использованием службы мгновенного обмена сообщениями.Двумя основными видами атак, основанными на использовании службы мгновенного обмена сообщениями, являются указание в теле сообщения ссылки на вредоносную программу и доставка самой программы. Конечно, мгновенный обмен сообщениями — это ещё и один из способов запроса информации. Одна из особенностей служб мгновенного обмена сообщениями — это неформальный характер общения. В сочетании

с возможностью присваивать себе любые имена, этот фактор позволяет злоумышленнику гораздо легче выдавать себя за другого человека и значительно повышает его шансы на успешное проведение атаки. Для получения надежного контроля над мгновенным обменом сообщениями в корпоративной среде следует выполнить несколько требований: выбрать одну платформу для мгновенного обмена сообщениями, определить параметры защиты, задаваемые при развертывании службы мгновенного обмена сообщениями, определить принципы установления новых контактов, задать стандарты выбора паролей, составить рекомендации по использованию службы мгновенного обмена сообщениями.

Список использованных источников:
1.Кузнецов, М. В.К89Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. — СПб.: БХВ-Петербург,2007. — 368 с.: ил.
2.http://www.kaspersky.by/
3.https://ru.wikipedia.org/

ПРОБЛЕМЫ ВНЕДРЕНИЯ И ИСПОЛЬЗОВАНИЯ НОВЫХ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ НА ПРЕДПРИЯТИИ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Ивановский А.Е., Солодовников А.Д.

Ермакова Е.В. – докт. экон. наук, доцент

Информационная технология — это цельная система методов и способов сбора, передачи, накопления, обработки, хранения, представления и использования информации. Современные информационные технологии непосредственно влияют на качество управленческих решений, на разработку планов, а часто и на способы производства продуктов и оказания услуг.

Сегодня практически невозможно обеспечить требуемое потребителями качество обслуживания и эффективность предприятия без применения информационных технологий, систем и программных комплексов для анализа, планирования и поддержки принятия коммерческих решений. Информационные технологи помогают предприятиям достигать поставленных целей, автоматизируя производственные процессы, обеспечивать выполнение стандартов, совершенствовать продукты на основе анализа спроса потребителей, снижать время изготовления продукции, сокращать сроки разработки проектов.

В современном бизнесе информационные технологии являются такой же важной составляющей предприятия, как стратегия, организационная структура, процессы, оргкультура и другие составляющие. Информационные технологии уже стали неотъемлемой частью общества, поэтому необходимо менять подходы к управлению организациями, так как изменились условия их функционирования в первую очередь за счет развития информационных технологий.

С помощью информационных технологий компании, как и ранее, рассчитывают улучшить свои показатели, однако сегодня в первую очередь все хотят большего объема продукции и его высокого качества за меньшие деньги. Поэтому перед руководителями компаний встает вопрос, разрабатывать ли программное обеспечение своими силами либо доверить этот вопрос посторонним фирмам. В подавляющем большинстве случаев решение принимается в пользу покупки программного обеспечения у сторонних фирм, специализирующихся на разработке информационных технологий.

В настоящее время сложилась четкая тенденция роста бизнеса в сфере аутсорсинга. На рисунках 1, 2 и 3 представлены ответы руководителей на различные вопросы об использовании ИТ-аутсорсинга:

Рис. 1 – Ответ руководителей на вопрос «Какие виды аутсорсинга используются в вашей компании?»

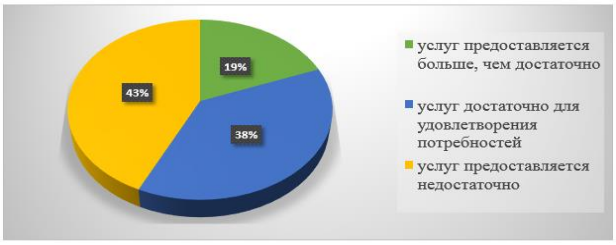

Рис. 2 – Ответ руководителей на вопрос «Достаточно ли услуг предлагается на отечественном рынке ИТ-аутсорсинга?»