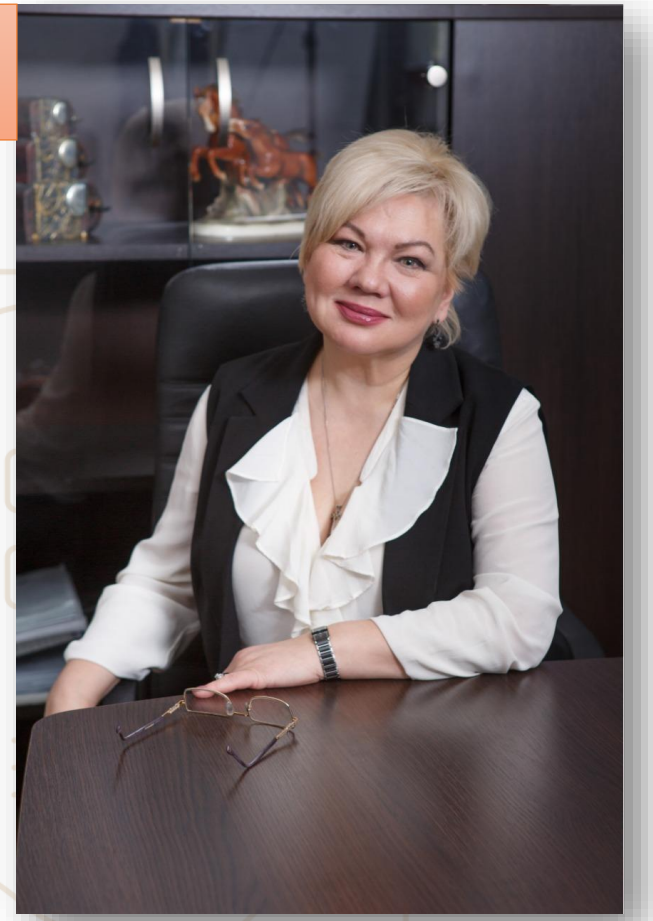
ФИНАНСОВЫЙ ЭКСПРЕСС

ИНФОРМАЦИОННАЯ (КИБЕРУГРОЗА) БЕЗОПАСНОСТИ БИЗНЕСА

ФИНАНСОВЫЙ ЭКСПРЕСС

ГААН ЕЛЕНА АЛЕКСЕЕВНА



- 25 лет в бизнесе, прошла все кризисы с кратным увеличением дохода
- Основатель и директор группы компаний «С-Лига»
- Аудитор, специалист по антикризисному управлению
- Автор семинаров и вебинаров по защите бизнеса от контролирующих органов
- Консультант по налогам
- Судебный эксперт
- Член Ассоциации Российских Детективов

ФИНАНСОВЫЙ ЭКСПРЕСС

Виды безопасности

- ***Экономическая (финансовая)****:безопасность, подразумевающая защищенность бизнеса, его прав и интересов от угроз со стороны внешних и внутренних факторов с помощью нормативно-правовых, организационных, технических, финансово-экономических и общественно-политических мероприятий*

- ***Информационная (кибербезопасность): это комплекс мер, которые защищают информацию и информационные системы от различных угроз, таких как несанкционированный доступ, взлом, потеря данных, нарушение конфиденциальности, целостности и доступности информации.***

- ***Правовая (юридическая):*** *комплекс мер по обеспечению интересов компании, направленный на разрешение возникших конфликтных ситуаций, а также на своевременное выявление, контроль и упреждение рисков юридического характера.*

ФИНАНСОВЫЙ ЭКСПРЕСС

Виды безопасности

- ***Кадровая безопасность:*** *комплекс мер по защите персональных данных сотрудников, контроль за выполнением трудовых обязанностей, предотвращение утечки коммерческой тайны и проверку кандидатов на работу на наличие судимостей и связей с преступными структурами. Предотвращение возможных внутренних угроз, связанных с действиями сотрудников (кадровый экстремизм)*

- ***Репутационная*** *—— вероятность изменения общественного мнения о компании в худшую сторону из-за тех или иных её действий или, наоборот, бездействия*

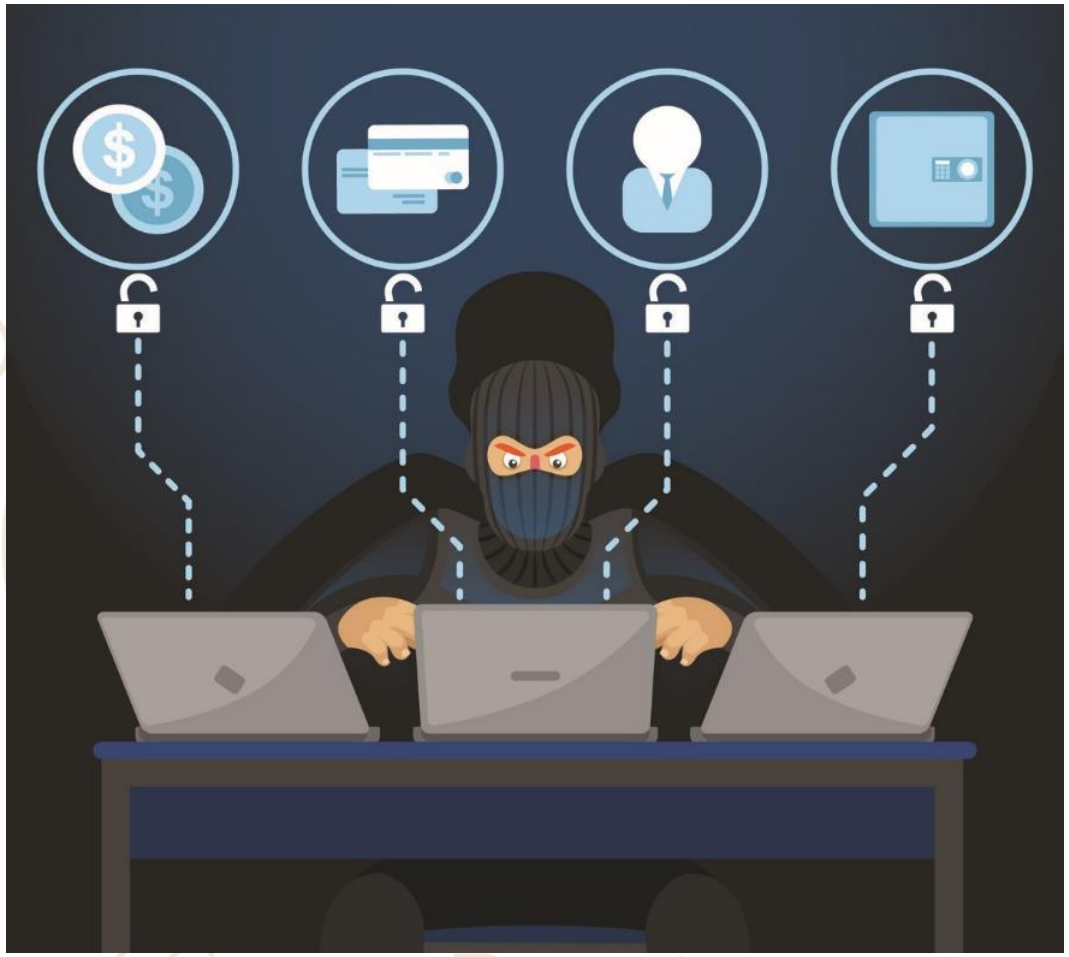
- ***Физическая****: обеспечение защиты имущества организации, её инфраструктуры, сотрудников, ограничение доступа посторонних лиц на территорию организации. Включает комплекс мер, направленных на защиту персонала, имущества, данных и физических активов от действий и событий, которые наносят ущерб или убытки организации.*

ФИНАНСОВЫЙ ЭКСПРЕСС

Информационная (кибербезопасность)

Это то, что обязательно необходимо любой современной компании

РИСКИ: вирусы в электронных письмах, проблемы с использованием облачных технологий или иных внешних сервисов, умышленное нанесение вреда кем-то из работников и многое другое



ФИНАНСОВЫЙ ЭКСПРЕСС

Внутренние угрозы ИБ

- **Преднамеренные** - сотрудники наносят организации вред сознательно (продают конфиденциальные сведения конкурентам). Причины могут быть в деньгах, желании отомстить компании за что-либо, политике компании в отношении коммерческой деятельности и т.д. Такие утечки наиболее опасны так как обусловлены умыслом на их совершение.
- **Непреднамеренные** - информацию повредили или удалили по ошибке. Произвели передачу (*копирование*) информации в мессенджер или на личную почту с целью поработать дома, не заблокировали компьютер, установили или полностью игнорировали парольную защиту, подключились к общедоступным сетям Wi-Fi, подключили личные аккаунты к корпоративному компьютеру и т.д.

ФИНАНСОВЫЙ ЭКСПРЕСС

Риски информационной безопасности бизнеса

К каким-либо секретным данным получили доступ третьи лица.

Кто же становится виновником подобных происшествий?

Инсайдер, завладевший ценными данными случайно.

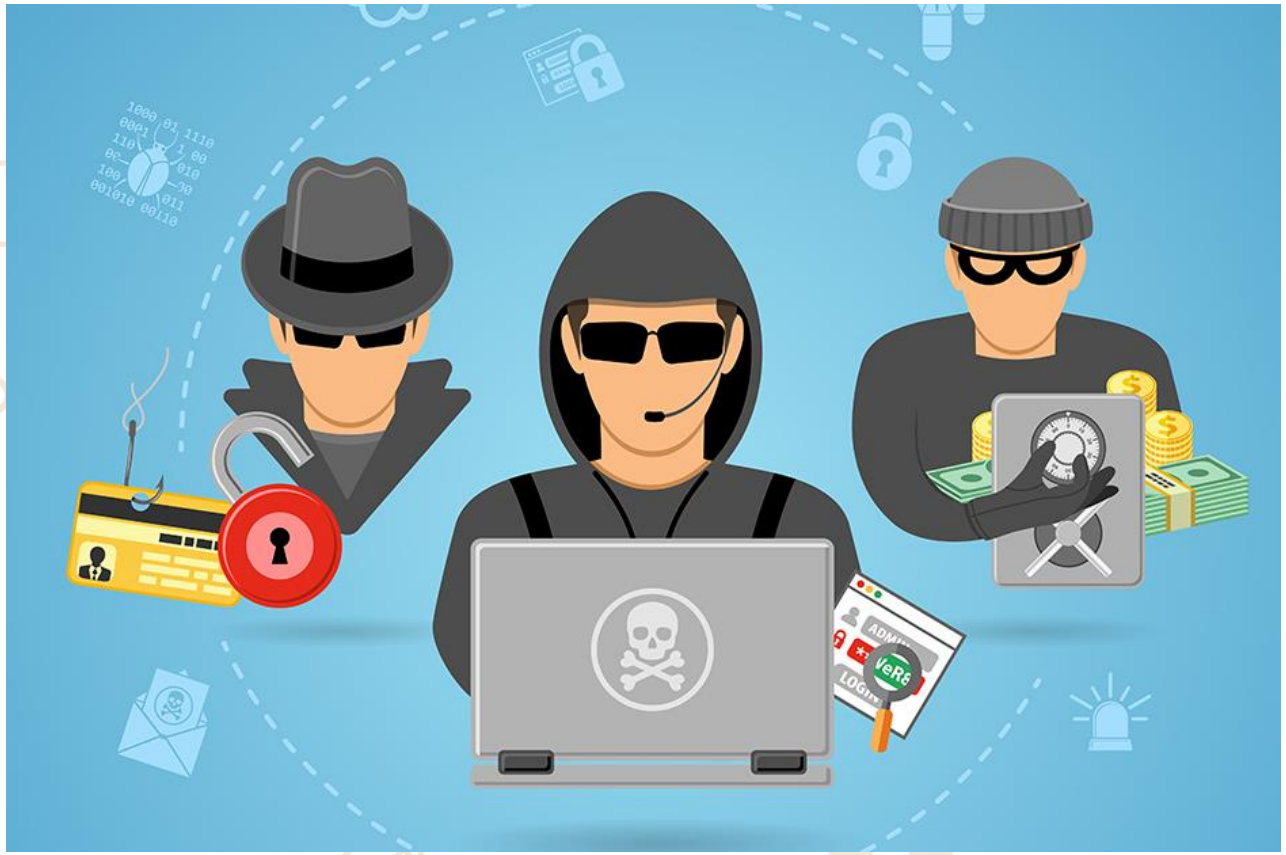
К примеру, сотрудник уже не работает в компании, но до увольнения он в рамках служебных обязанностей имел доступ к секретной информации. И человек мог скачать некие конфиденциальные сведения на свой компьютер просто в спешке, по невнимательности. В принципе сама по себе такая утечка не опасна для бизнеса, ведь никто не планировал сливать на сторону полученные данные с целью наживы, из мести или по иным причинам.

Нужно позаботиться о том, чтобы ничего подобного происходить не могло даже по неосторожности. Вирусная активность сейчас достигает таких размахов, что злоумышленники при желании найдут способ добраться до информации, вышедшей за пределы компании

ФИНАНСОВЫЙ ЭКСПРЕСС

Риски информационной безопасности бизнеса

Инсайдер, запланировавший злой умысел.
Это сотрудники, которые покидали компанию, затаив обиду. Такой человек может намеренно задумать информационную диверсию, чтобы навредить репутации фирмы, нанести ей финансовый урон. Сведения он добывает, воспользовавшись личным уровнем доступа или через дружественно настроенных коллег. А полученные данные можно потом использовать, например, как инструмент шантажа (пообещать поделиться ими с конкурирующими фирмами или предать гласности и т. п.).



ФИНАНСОВЫЙ ЭКСПРЕСС

Риски информационной безопасности бизнеса

Сторонний злоумышленник, *некто, никак не связанный с компанией, но планирующий завладеть её конфиденциальной информацией. К примеру, хакер (с целью наживы), либо ушлый подросток (пробующий свои силы в IT, взламывая чужие базы данных) и др.*
Если в информационных системах компании есть достаточно серьезные уязвимости, то вероятность утечки корпоративных данных, разумеется, возрастает.

Причины:

- *недостаточно надежные программные и программно-аппаратные базы,*
- *слабые коды, которые нарушители легко преодолевают (и получают доступ к секретным сведениям).*

Защитные обновления и патчи выходят довольно часто, производители за этим следят, заботясь о безопасности бизнеса своих клиентов. И всё же случается, что хакеры успевают узнать об уязвимости раньше разработчиков ПО и быстренько сделать соответствующий эксплойт.

ФИНАНСОВЫЙ ЭКСПРЕСС

Основные причины утечек информации

- ***Слишком много прав доступа у инсайдеров.*** Когда большое число людей имеет допуск к конфиденциальным данным, риск утечек возрастает. Как уже упоминалось выше, зачастую именно через инсайдеров (из-за их невнимательности либо злонамеренности) информация уходит налево.
- ***Вирусы в ПО***. Вредоносные программы, внедренные в корпоративную инфраструктуру, открывают пути для утечки, повреждения, воровства данных, могут вообще вывести из строя IT-систему. В связи с этим для компании возрастает риск получения значительного финансового и имиджевого ущерба.
- ***Спланированные атаки.*** Злоумышленники не обязательно ставят перед собой цель взломать базу данных конкретной компании. Они могут просто рандомно искать слабые места в защите той или иной инфраструктуры. Но бывают и целенаправленные «набеги», с применением хитрых особых методов вроде писем с электронных адресов сотрудников этой же фирмы, дипфейков с участием первых лиц компании и т. п.

ФИНАНСОВЫЙ ЭКСПРЕСС

Основные причины утечек информации

- ***Фишинг, спуфинг***. Отправка писем с почты людей, которым получатель доверяет (например, это может быть начальник отдела). Хакеры таким образом подталкивают человека скачать, например, вложение с вирусом, открыть вредоносную ссылку, переслать какие-то важные данные и т. п. То есть адресат заглатывает наживку в виде такого письма и потом своими действиями помогает злоумышленникам.
- ***Доступ к учетным записям работников компании.*** Сотрудник, попавшийся на крючок в результате фишинга, сам того не зная, может теперь открыть для злоумышленников свою рабочую учетную запись. Хакерам достаточно переслать ему письмо, отправленное как бы с корпоративной почты и содержащее в себе ссылку (тоже типа на корпоративный сайт). Кликнув по ней, получатель оказывается на странице авторизации, где требуется введение логина и пароля, которые мгновенно оказываются в распоряжении злоумышленников.
- ***Ненадежные пароли, повторное их применение***. Простыми шифрами легче пользоваться, поэтому часто сотрудники задействуют именно их. Но базы паролей могут сливаться, например, через форумы или через старую взломанную почту и т. п. А дальше подобрать credentials и войти в вашу учетную запись – для злоумышленников задача более чем простая.

ФИНАНСОВЫЙ ЭКСПРЕСС

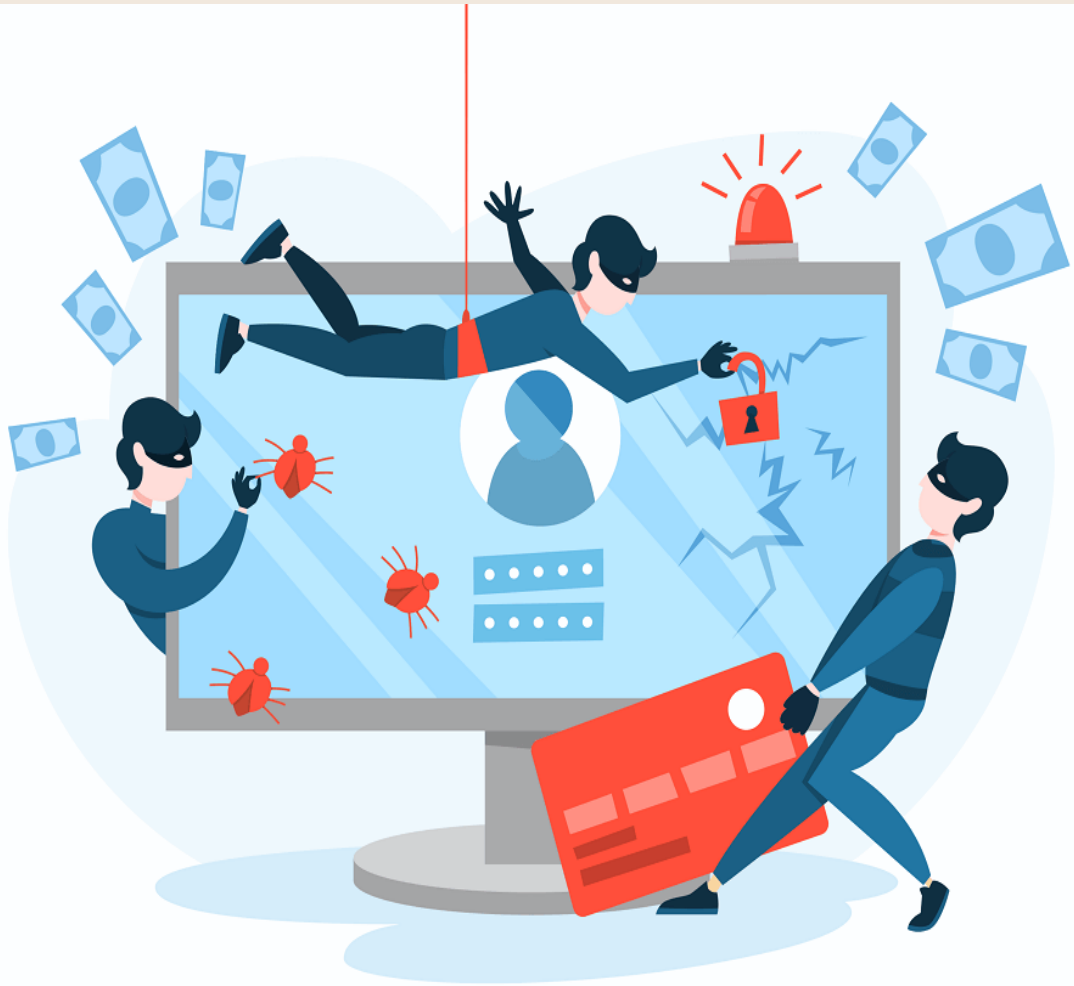
Предотвращение утечек

Пути попадания ценной информации в руки посторонних:

• *целенаправленная кража (шпионская, со стороны инсайдеров, рейдеров);*

• *невнимательность своих же сотрудников (отправка пароля в электронном письме, открытие вирусных ссылок, утеря носителя с ценными данными, отсутствие контроля прав доступа и т. п.).*

Применяется техника для уничтожения информации, данные зашифровывают, хранят на серверах других стран и т. п.



ФИНАНСОВЫЙ ЭКСПРЕСС

Предотвращение утечек

С невнимательностью персонала обычно борются так: **сокращают до возможного минимума права доступа к корпоративным данным, налагают на сотрудника индивидуальную ответственность, строго регламентируют работу с важной документацией и носителями информации (которыми пользуются работники), передачу ценных сведений осуществляют только по защищенным каналам.**

Также информационной безопасности бизнеса поспособствует запись телефонных переговоров, внедрение RMS и DLP, использование зашифрованных USB-карт, отслеживание трафика, наблюдение за персоналом в ходе работы за ПК и т. п.

ФИНАНСОВЫЙ ЭКСПРЕСС

Обеспечение информационной безопасности бизнеса

Проблемы безопасности связаны именно с недостаточно надежной системой информационной защиты. Это факт, подтвержденный статистикой. Допускаются утечки, секретные данные теряются, попадают в руки к конкурентам, злоумышленникам. Задача IT-специалистов – принять достаточные защитные меры для снижения рисков, способных нанести урон бизнесу.

В первую очередь важно защитить финансовую информацию, далее – не допустить утечки данных, и третье – предотвратить DDoS-атаки. Первые две задачи давно уже занимают лидирующие позиции, а вот третья – это, так сказать, новинка в списке подобных проблем.

1. *DDoS-атаки-это тип атаки на компьютерные системы, при которых ресурс становится недоступным для нормального использования. Целевая система или сервис перегружаются, чтобы они не могли обрабатывать входящие запросы.*

2. *DoS-атака исходит от одного источника, например, от одного компьютера, который отправляет массу запросов к целевому ресурсу. Это может выявить уязвимости на целевом ресурсе или просто привести к переполнению буфера.*

Атаки все чаще и чаще предпринимаются в направлении именно малого и среднего предпринимательства.

Если говорить о российских компаниях, то в рамках повышения безопасности бизнеса самые распространенные меры такие: управление приложениями, обновлениями, сетевой структурой, контроль вирусного ПО, отслеживание использования внешних сервисов и мобильников.

Следует уделять внимание защищенности денежных переводов и т. д. и т. п.

ФИНАНСОВЫЙ ЭКСПРЕСС

Основные методы обеспечения информационной безопасности бизнеса

Предотвращение вторжений: Осуществляется с помощью специального программного и аппаратного обеспечения для мониторинга поступающего трафика. Как только фиксируется нападение, доступ тут же блокируется системой, а к ответственному сотруднику приходит сообщение об опасности.

Обеспечить защиту от вторжений можно двумя способами:

1. ***С помощью IPS.*** Данная система блокирует любую подозрительную активность и тщательно просеивает трафик, отметая всё лишнее. Система хороша тем, что и обнаруживает, и предотвращает угрозы. Из минусов – IPS часто срабатывает не по делу. Администратору приходится на это отвлекаться, запускать проверку, останавливать на время работу сети.
2. ***С помощью IDS.*** Система замечает подозрительную активность и оповещает ответственного сотрудника. Из плюсов данного способа – вторжения отслеживаются весьма эффективно, а дальнейшие решения по ним принимает уже администратор. Отрицательный момент состоит в том, что если этот специалист не сработает достаточно оперативно, система может быть серьезно повреждена.

ФИНАНСОВЫЙ ЭКСПРЕСС

Информационная (кибербезопасность)

<u>Участились случаи мошеннических рассылок от имени руководителей компаний.</u>

Злоумышленники узнают из открытых источников о структуре менеджмента компании и создают фейковые учетные записи, с которых отправляют сообщения. При этом они пытаются вызвать ощущение важности и срочности, не оставляя времени на размышления.

Чаще всего пишут письмо от имени генерального директора. Но сам руководитель никаких поручений и заданий не дает. Он просто предупреждает, что сейчас перезвонит человек из госорганов, которому нужно получить информацию, и просит оказать ему содействие.

Мошенники пишут в Telegram, могут звонить с незнакомых номеров. Самое главное, что должно насторожить – это срочность.

<u>Слова-маркеры: «срочно», «немедленно», «обязательно».</u>

ФИНАНСОВЫЙ ЭКСПРЕСС

Защита файлов с ценной информацией

Речь идет об информации, хранящейся на принадлежащих компании компьютерах и серверах. Способы для защиты файлов есть следующие:

- ***шифрование данных (с помощью EFS, Qnap, CryptoPro и т.п.);***
- ***шифрование используемых персоналом гаджетов****: мобильных телефонов, ноутбуков, любых носителей (с помощью специальных программ вроде Kasperskiy, SecretDisk, Endpoint Encryption или модулей шифрования, выпускаемых компаниями Sony, Asus и иными);*
- ***шифрование данных от сисадмина*** *(применяется TrueCrypt);*
- ***обязательная регистрация мобильных телефонов через трекеры систем мониторинга*** *(задействуется ПО Касперского или Prey);*
- ***полное или частичное закрытие доступа к определенным файлам*** *(в качестве инструмента здесь хорошо себя зарекомендовал Active Directory Rights Management Services);*
- ***применение единой аутентификации****. Тут на выбор можно привязать аппаратуру к структуре домена (доменная авторизация) и использовать электронный ключ (E-token), либо применять систему СМС-оповещений.*

ФИНАНСОВЫЙ ЭКСПРЕСС

Защита 1С и оптимизация работы с данным ПО

Меры:

• *для базы 1С: использование специальных защитных систем шифрования дисков, систем для обмена файлами и ценными сведениями, минимизация прав доступа к ним;*

• *для СУБД базы 1С: применение шифрования, запрет или минимизация прав доступа к серверам (как электронного, так и физического), уменьшение объемов административных прав (для персонала) и т. п.*

• *защита секретной корпоративной информации.*

Меры, способствующие информационной безопасности бизнеса:

-защита корпоративных каналов взаимодействия;

-оперативное удаление данных с сервера;

-мониторинг работы персонала;

-организация бесперебойного функционирования бизнес-процессов,

- обеспечение их высокой отказоустойчивости.

ФИНАНСОВЫЙ ЭКСПРЕСС

Как противостоять киберугрозе

1. Определите, кто отвечает за ИБ в организации
2. Обучайте сотрудников
3. Тестируйте продукты, чтобы найти уязвимости
4. Применяйте только официальное программное обеспечение
5. Используйте антивирусное ПО
6. Используйте двухфакторную аутентификацию для доступа ко всем тем ресурсам, где можно ее настроить
7. Разработайте парольную политику
8. Шифруйте важные данные на дисках, в папках и на сменных носителях
9. Создавайте резервные копии важных файлов

ФИНАНСОВЫЙ ЭКСПРЕСС

Социальная инженерия

В контексте информационной безопасности — **психологическое манипулирование людьми с целью совершения определенных действий или разглашения...**

Информация, которую ищут преступники, может быть разной, но чаще всего это банковские реквизиты, а также пароли от учётных записей. Кроме того, преступники могут попытаться получить доступ к компьютеру жертвы, чтобы установить там вредоносное программное обеспечение, помогающее извлекать любую информацию.

ФИНАНСОВЫЙ ЭКСПРЕСС

Примеры социальной инженерии

❖**Плечевой серфинг-** *разновидность техники социальной инженерии, которая заключается в наблюдении личной информации жертвы через её плечо.*

Этот тип атаки распространён в общественных местах, таких как кафе, торговые центры, аэропорты, вокзалы, а также в общественном транспорте.

Цель плечевого серфинга — *получение таких конфиденциальных данных, как личные идентификационные номера (PIN-коды), пароли и другие. Неавторизованные пользователи отслеживают нажатия клавиш, вводимые на устройстве, или прослушивают произносимую конфиденциальную информацию.*

Опасность плечевого серфинга заключается в том, что злоумышленникам необходим только один удачный момент, чтобы увидеть нужное сообщение и получить доступ к данным пользователя.

ФИНАНСОВЫЙ ЭКСПРЕСС

Примеры социальной инженерии

❖**Претекстинг** - *когда злоумышленник убеждает цель раскрыть конфиденциальную информацию или отправить ему деньги, придумав историю. Может осуществляться в различных формах, включая телефонные звонки, текстовые сообщения, электронные письма или даже личные встречи. Перед атакой злоумышленник собирает как можно больше информации о своей цели. Затем, он пытается убедить жертву, что он ее знакомый.*

Добыв информацию, необходимую для атаки, злоумышленники планируют, за кого они будут себя выдавать и какую историю будут рассказывать, чтобы убедить потенциальную жертву

Распространенные типы претекстинга

- Пожилые родственники
- Сайт знакомств
- Руководители

ФИНАНСОВЫЙ ЭКСПРЕСС

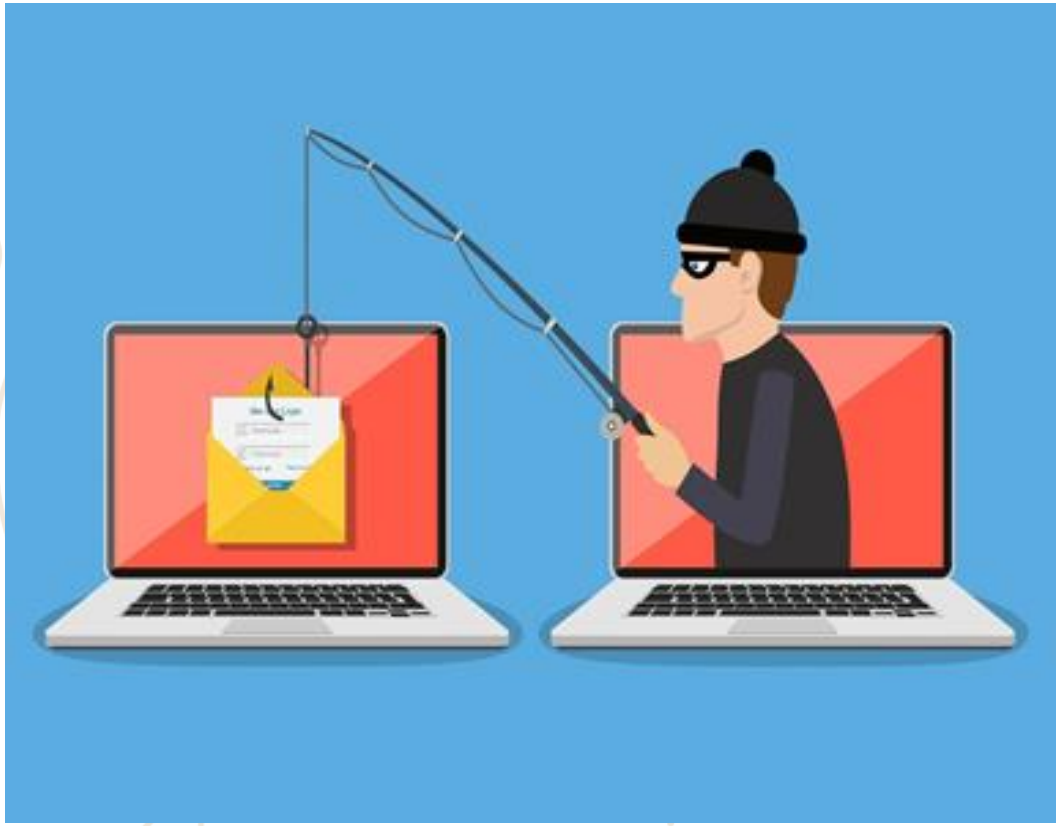
Примеры социальной инженерии

❖ **Фишинг-** *это попытка мошенников получить конфиденциальную информацию, маскируясь под доверенное лицо.*

Злоумышленник может выдать себя за представителя банка, менеджера службы поддержки, коллегу или друга, чтобы заставить жертву загрузить вирус на устройство или перенаправить на мошеннический сайт. Там у жертвы будут украдены личные данные — логины и пароли, данные кредитных карт и номера телефонов.

Примеры фишинга:

- *подозрительное письмо с просьбой сообщить номер банковского счёта;*
- *голосовое сообщение с предупреждением о краже личных данных;*
- *заманчивое предложение в социальных сетях.*



ФИНАНСОВЫЙ ЭКСПРЕСС

Примеры социальной инженерии

❖**Заражение ПК вредоносным ПО**

Признаки заражения компьютера вирусом

1.Снижение производительности компьютера. *Если компьютер стал работать медленнее, задержки и зависания стали частым явлением, это может быть признаком наличия вируса.*

2.Появление непонятных сообщений и рекламы. *Если стали замечать странные сообщения, окна с рекламой или спамом, то компьютер, скорее всего, заражён вирусом.*

3.Изменения в настройках системы. *Если без вашего согласия произошли изменения в настройках компьютера, например, автоматическое отключение антивирусных программ или брандмауэра, то возможно, вы заразились вирусом.*

4.Неожиданный запуск программ. *Если на рабочем столе или в панели задач появились незнакомые ярлыки или запущены неизвестные программы, то это может свидетельствовать о наличии вирусного загрязнения.*

ФИНАНСОВЫЙ ЭКСПРЕСС

Примеры социальной инженерии

❖**Обратная социальная инженерия -** *это вид атаки, при котором жертва сама обращается к злоумышленнику и предоставляет ему нужные сведения.*

- ***Внедрение особого ПО.*** *Поначалу программа или система работает исправно, но потом происходит сбой, требующий вмешательства специалиста.*
- ***Реклама.*** *Злоумышленники могут рекламировать свои услуги как компьютерных мастеров или других специалистов.*
- ***Помощь****. Социальный инженер может умышленно оказаться в числе тех, к кому обратятся за помощью в случае сбоя.*

Для защиты от социальной инженерии рекомендуется проявлять разумный скептицизм и бдительность.

ОБРАТНАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Жертва сама предлагает нужную информацию злоумышленнику (лицу, обладающему авторитетом в технической или социальной сфере, которое часто получает важную личную информацию, в том числе, когда никто не сомневается в их порядочности: сотрудники службы поддержки никогда не спрашивают у пользователей идентификатор или пароль – им не нужна эта информация – однако, многие пользователи ради скорейшего устранения проблем добровольно сообщают эти сведения).

ПРИЗНАКИ

Злоумышленник, работающий вместе с жертвой, изменяет на её компьютере имя файла или перемещает его в другой каталог	Жертва замечает пропажу файла. Злоумышленник заявляет, что может все исправить, но только войдя в систему с учетными данными жертвы. Жертва, желая быстрее завершить работу или избежать наказания за утрату информации, соглашается.	Жертва просит злоумышленника войти в систему под её именем, чтобы попытаться восстановить файл	Злоумышленник: неохотно соглашается и восстанавливает файл; крадет идентификатор и пароль жертвы; успешно осуществив атаку, улучшает свою репутацию, и вполне возможно, что после этого к нему будут обращаться за помощью и другие коллеги. Этот подход не пересекается с обычными процедурами оказания услуг поддержки и осложняет поимку злоумышленника

НЕСАНКЦИОНИРОВАННОЕ ПРОНИКНОВЕНИЕ

получение злоумышленником физического доступа на объект путем принуждения или обмана сотрудников, или в обход периметра безопасности	получение злоумышленником конфиденциальных данных и (или) установка крытых устройств съема информации в очень короткий промежуток времени	фотографирование документов, оставленных на принтерах или столах, или установка устройств, обеспечивающих последующий Wi-Fi или 3G доступ к сети

ФИНАНСОВЫЙ ЭКСПРЕСС

ВЫВОД

Тот, кто почуял ветер перемен, должен строить не щит от ветра, а ветряную мельницу.

В том, что с нами происходит, виноваты мы сами

ФИНАНСОВЫЙ ЭКСПРЕСС

Вы можете связаться со мной:

Тел: 8 - 905-968-85-94
Почта: elena_gaan@mail.ru
Телеграмм:
PROбизнес и налоги
PROбизнес и финансы