Информационная безопасность в самом широком смысле – это совокупность средств защиты информации от случайного или преднамеренного воздействия. Независимо от того, что лежит в основе воздействия: естественные факторы или причины искусственного характера – владелец информации несет убытки.

В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы:

- внутренние угрозы

- внешние угрозы

- атаки на АСУТП

- информационные атаки и войны

ВНУТРЕННИЕ УГРОЗЫ И УТЕЧКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

Внутренние угрозы – это угрозы, которые исходят от сотрудников компании

и наносят ей ущерб в результате кражи корпоративной информации или

ее утечки по неосторожности, а также коррупции, мошенничества, сговоров,

воровства и саботажа.

Пример:

В Болгарии был арестован специалист по информационной безопасности, которого обвинили в краже персональных данных и финансовых данных 5 миллионов граждан из Национального налогового агентства (NRA). Об этом 25 июля 2019 года сообщили в Panda Security. По заключению компании, этот инцидент стал самым крупным нарушением данных в Болгарии с населением около 7 миллионов человек.

«Синдром Клинтон», сентябрь 2016. Хиллари Клинтон было не всегда удобно вести переписку, используя рабочую почту, поэтому она пересылала письма, содержащие конфиденциальную информацию, по внешней почте. Кроме того, опасаясь хранить важную переписку у себя, она организовала хранение рабочих писем Госдепартамента США на личном сервере. В итоге эти действия привели к утечке информации, составляющей гостайну.

КАК ЗАЩИЩАТЬСЯ ОТ ВНУТРЕННИХ УГРОЗ И УТЕЧЕК ИНФОРМАЦИИ?

1. Для персонала – соблюдение правил обращения с информацией (запрет на использование публичной почты для передачи конфиденциальной информации, выключать компьютеры и ноутбуки при отсутствии на рабочем месте, не разглашать информацию в соцсетях)

2. Для организации - установка правил обращения с информацией и контроль за их соблюдением (составление положения о коммерческой тайне и защите персональных данных, выбор и назначение сотрудников ответственных за безопасность, разработка разного рода процедур по защите информации)

ВНЕШНИЕ УГРОЗЫ И ЦЕЛЕВЫЕ АТАКИ

Целевые атаки – это заранее спланированные действия по атаке на ИТ-системы конкретной организации. У каждой атаки есть заказчик, исполнитель, объект-жертва и цель.

ОТЛИЧИЕ ЦЕЛЕВЫХ АТАК ОТ ВИРУСОВ:

- Использование нескольких векторов нападения одновременно

- Использование методов социальной инженерии1

- Заранее произведена «разведка» – получена информация об инфраструктуре предприятия, используемых методах и средствах защиты

- Как правило, происходит отключение используемой защиты

- Часто целевая атака начинается с DDoS-атаки2

- Вредоносный код, как правило, внедряется по частям

1. Социальная инженерия – это метод несанкционированного доступа к информации, основанный на использовании слабостей человеческого фактора и без использования технических средств. Злоумышленник получает информацию, например, с помощью обычного телефонного звонка или путем проникновения в организацию под видом ее служащего.

2. DDoS-атака (Distributed Denial of Service) – это атака на веб-ресурс, основной целью которой является выведение его из строя путем подачи большого количества ложных запросов, которые сервер не успевает обрабатывать, и сайт становится недоступным для пользователя.