Основы информационной безопасности

1

Теория

Что такое и зачем нужна информационная безопасность

2

Основы

Существующие требования

3

Техника

Обзор практики применения технических решений

4

Практика

От теории к делу

digital academy

Содержание

digital academy

Информационная безопасность

состояние защищенности информационной среды

Защита информации - действия по предотвращению возможного повреждения или уничтожения информации, а также несанкционированного доступа к ней (но вместе с тем – обеспечение беспрепятственного доступа к информации со стороны легитимных пользователей)

digital academy

Основные составляющие информационной безопасности+

Конфиденциальность - это гарантия, что информация может быть прочитана и проинтерпретирована только теми людьми и процессами, которые авторизованы это делать. Обеспечение конфиденциальности включает процедуры и меры, предотвращающие раскрытие информации неавторизованными пользователями. Информация, которая может считаться конфиденциальной, также называется чувствительной. Примером может являться почтовое сообщение, которое защищено от прочтения кем бы то ни было, кроме адресата.

Доступность - это гарантирование того, что авторизованные пользователи могут иметь доступ и работать с информационными активами, ресурсами и системами, которые им необходимы, при этом обеспечивается требуемая производительность. Обеспечение доступности включает меры для поддержания доступности информации, несмотря на возможность создания помех, включая отказ системы и преднамеренные попытки нарушения доступности. Примером может являться защита доступа и обеспечение пропускной способности почтового сервиса

Целостность - это гарантирование того, что информация остается неизменной, корректной и аутентичной. Обеспечение целостности предполагает предотвращение и определение неавторизованного создания, модификации или удаления информации. Примером могут являться меры, гарантирующие, что почтовое сообщение не было изменено при пересылке.

digital academy

Виды угроз безопасности информации

- Хищение(копирование информации)
- Уничтожение
- Модификация(искажение)
- Нарушение доступности(блокировка)
- Отрицание подлинности информации
- Навязывание ложной информации

digital academy

Угрозы по аспекту ИБ

- Угроза нарушения доступности - заключается в том, что информация становится доступной лицам, не имеющих полномочия
- Угроза нарушения целостности - любое умышленное изменение информации, хранящейся в системе
- Угроза нарушения конфиденциальности - возникает в результате несанкционированных и непреднамеренных воздействий, блокируется доступ к некоторому информионному ресурсу

digital academy

Риски

Риски - потенциальная опасность нанесения ущерба организации в результате реализации некоторой угрозы с использованием угрозы с использованием уязвимости актива или группы активов. Определяется как сочетание вероятности события и его последствий

Оценка - процесс состоящий из идентификации, анализа и оценивания

Анализ - систематический процесс определения величины риска

digital academy

Возможные защитные меры

Ликвидация риска - ликвидация источника/уязвимости

Уменьшение риска - повышение уровня безопасности

Принятие риска - смирение и разработка

Переадресация риска - заключение страхового договора

digital academy

Пример из жизни

табличка оценка рисков

digital academy

Меры по обеспечению информационной безопасности

Технические

Аппаратные, программные средства и технологии защиты от вредоносных программ, внешних сетевых атак и пр. (в том числе антивирусные программы)

Правовые

Совокупность нормативных и правовых актов, регулирующих вопросы защиты информации

Правовые основы информационной безопасности

Наказания за создание вредоносных программ:

штраф и конфискация компьютерного оборудования

тюремный срок

смертная казнь (Филиппины)

digital academy

Основы лицензионной политики в сфере распространения программ и данных

Лицензия (пользовательская лицензия)-набор правил распространения, доступа
и использования информации, устанавливаемый(в рамках, допустимых законом) собственником программы - ее создателем или продавцом.

Лицензионная политика-комплексный механизм, определяющий всю совокупность условий предоставления той или иной программы пользователям, включая систему ценовых скидок и оговоренные в лицензии ограничения и специальные условия ее использования

digital academy

Виды ПО

Открытое

- Коммерческое: Пробное (trial) и демо-версии(demo)
- Условно-бесплатное (shareware)
- Бесплатное(freeware)

Свободное

- Свободное (free software)
- Открытое (open source)

Google Chrome

VLC Player

digital academy

Угрозы при использовании нелицензионного ПО

Нелицензионное (пиратское) ПО - программное обеспечение, полученное и/или используемое незаконным способом, т. е. в нарушение правил пользовательской лицензии (как правило, от третьих лиц или через третьих лиц, не имеющих прав на распространение такой программы)

- Распространение и использование нелицензионного ПО является нарушением Закона об охране авторских прав, за что виновный несет гражданскую, административную или уголовную ответственность
- Хакеры используют «взломанные» программы в качестве «приманки», встраивая в них «троянские программы»
- Сайты и диски, посредством которых программами распространяются «взломанные» программы либо средства для их «взлома», бывают заражены различными вредоносными

digital academy

Четыре советов по безопасности при работе на общедоступном компьютере:

1. не сохраняйте свои учетные данные для входа в систему,

2. не оставляйте без присмотра компьютер с важными сведениями на экране;

3. опасайтесь подглядывания через плечо;

4. не вводите важные сведения на общедоступном компьютере.

Практическое задание

digital academy

Полезные ссылки

https://www.youtube.com/watch?v=3-X-FVXv1yg

https://www.youtube.com/watch?v=39-G3FUglsg

digital academy

Спасибо за внимание!

Присоединяйтесь к нам

Telegram

Facebook

Instagram

info@digitalacademy.kg
Юнусалиева 173/2
0(990)037-037

digital academy