Научная библиотека Государственного образовательного учреждения высшего образования Луганской Народной Республики «Донбасский государственный технический институт»

Безопасность информации

30 ноября Всемирный день Защиты информации

Информационная безопасность (англ. Information Security, а также — англ. InfoSec) — практика предотвращения несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

- **Основная задача информационной безопасности — сбалансированная защита конфиденциальности, целостности и доступности данных, с учётом целесообразности применения и без какого-либо ущерба производительности организации.**

Перевод большинства информационных архивов, денежных средств и коммуникаций в электронную форму создал самостоятельный тип актива – ***информацию***

Как любая ценность, она подвергается посягательствам со стороны различных мошенников

Страдают от преступлений, совершаемых в информационной сфере, и граждане

Большинство людей так, или иначе испытывают на себе воздействие угроз информационной безопасности:

- ***вредоносных программ***

(вирусов и червей, троянских программ, программ-вымогателей)

- ***фишинга или кражи личности***

(представляет собой мошенническую попытку завладения конфиденциальной информацией - например, учётной записью, паролем или данными кредитной карты)

Обычно пользователя Интернета стараются заманить на мошеннический веб-сайт, неотличимый от оригинального сайта какой-либо организации (банка, интернет-магазина, социальной сети и т. п.)

Как правило, такие попытки совершаются с помощью массовых рассылок поддельных электронных писем якобы от имени самой организации, содержащих ссылки на мошеннические сайты.

Открыв такую ссылку в браузере, ничего не подозревающий пользователь вводит свои учётные данные, которые становятся достоянием мошенников!!!


•Снижение — внедрение мер безопасности и противодействия для устранения уязвимостей и предотвращения угроз;
Основными способами противодействия угрозам информационной безопасности или информационным рискам являются:
отказ — отказ от чрезмерно рисковой деятель-ности
передача — перенос затрат, связанных с реализацией угроз на третьих лиц: страховые или аутсорсинговые компании;
принятие — формирование финансовых резервов в случае, если стоимость реализации мер безопасности превышает потенциальный ущерб от реализации угрозы;

Программно-аппаратные средства системы обеспечения информационной безопасности

Средства защиты от несанкционированного доступа

Средства авторизации;
мандатное управление доступом;
избирательное управление доступом;
управление доступом на основе ролей;
журналирование.

Системы предотвращения утечек конфиденциальной информации (DLP-системы)

Анализаторы протоколов;
антивирусные средства;
межсетевые экраны;
криптографические средства;
шифрование;
цифровая подпись;
системы резервного копирования .

Системы Аутентификации

Пароль;
ключ доступа (физический или электронный);
сертификат;
биометрия;
инструментальные средства анализа систем защиты;
антивирус.

Методы защиты:

препятствие на пути предполагаемого похитителя, которое создают физическими и программными средствами

маскировка, или преобразование данных, обычно – криптографическими способами

управление, или оказание воздействия на элементы защищаемой системы

регламентация, или разработка нормативно-правовых актов,

принуждение, или создание таких условий, при которых пользователь будет вынужден соблюдать правила обращения с данными;

побуждение, или создание условий, которые мотивируют пользователей к должному поведению.

Основные принципы защиты информации:

Конфиденциальность - информации достигается предоставлением к ней доступа с наименьшими привилегиями исходя из принципа минимальной необходимой осведомлённости Иными словами, авторизованное лицо должно иметь доступ только к той информации, которая ему необходима для исполнения своих должностных обязанностей.

Целостность - Чёткое осуществление операций или принятие верных решений в организации возможно лишь на основе достоверных данных, хранящихся в файлах, базах данных или системах, либо транслируемых по компьютерным сетям. Иными словами, информация должна быть защищена от намеренного, несанкционированного или случайного изменения.

Доступность - Согласно этому принципу, информация должна быть доступна авторизованным лицам, когда это необходимо.

Спасибо за внимание!

Добро пожаловать в Научную библиотеку ДонГТИ

обзор подготовила библиотекарь Сергеева Е.В.

наш адрес: ЛНР, г. Алчевск, ул. Ленинградская, 45-а,
http://library.dstu.education/