Информационная безопасность

Работу выполнили:
Константин Ходовцев
Никита Загвоздкин
Алёна Савченко

Поняти

Информационная безопасность – это защита информации и информационных систем от неавторизованного доступа, использования, раскрытия, искажения, изменения или уничтожения в целях обеспечения конфиденциальности, целостности и доступности

Защита данных призвана обеспечить оперативный доступ к информации. Информационная безопасность должна предусмотреть возможные угрозы и подтвердить юридическую значимость сведений, которые хранятся или перед

Ключевые принципы

В 1975 году Джерри Зальцер и Майкл Шредер в статье «Защита информации в компьютерных системах» впервые предложили разделить нарушения безопасности на три основных понятия:

1. *Конфиденциальность* (*Confidentiality на англ.)*— подразумевает под собой обеспечение доступа к информации только авторизованным пользователям.
2. *Целостность* (*Integrity* с англ.) — это обеспечение достоверности и полноты информации.
3. *Доступность* (*Availability* с англ.) — свойство быть доступным и готовым к использованию по запросу авторизованного субъекта.

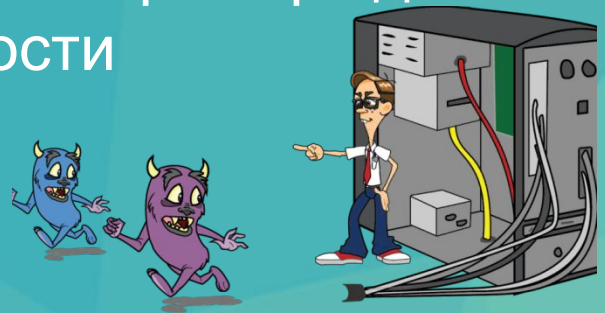
В совокупности эти три ключевых принципа информационной безопасности именуются триадой CIA. Исходя из ваших целей и выполняемых задач на виртуальном сервере, необходимы будут и различные меры и степени защиты, применимые по каждому из этих трех пунктов.

Конфиденциальность

Авторизованное лицо должно иметь доступ только к той информации, которая ему необходима для исполнения своих должностных обязанностей. Упомянутые выше преступления против неприкосновенности частной жизни, такие, как кража личности, являются нарушениями конфиденциальности.

Одной из важнейших мер обеспечения конфиденциальности является классификация информации, которая позволяет отнести её к строго конфиденциальной, или предназначенной для публичного, либо внутреннего пользования.

Шифрование информации — характерный пример одного из средств обеспечения конфиденциальности



Целостность

Информация должна быть защищена от намеренного, несанкционированного или случайного изменения по сравнению с исходным состоянием, а также от каких-либо искажений в процессе хранения, передачи или обработки. Однако её целостности угрожают компьютерные вирусы и логические бомбы, ошибки программирования, неавторизованный доступ и тому подобное.

Помимо преднамеренных действий, во многих случаях неавторизованные изменения важной информации возникают в результате технических сбоев или человеческих ошибок по оплошности.
Например, к нарушению целостности ведут: случайное удаление файлов, ввод ошибочных значений, изменение настроек, выполнение некорректных команд, причём, как рядовыми пользователями, так и системными администраторами. Для защиты целостности информации необходимо применение множества разнообразных мер контроля и управления изменениями информации и обрабатывающих её систем. Типичным примером таких мер является ограничение круга лиц с правами на изменения лишь теми, кому такой доступ необходим для выполнения служебных обязанностей. Любые действия, влекущие изменения, должны быть обязательно протоколированы.

Доступность

Основными факторами, влияющими на доступность информационных систем, являются DoS-атаки (аббревиатура от *Denial of Service* с англ. — «отказ в обслуживании»), атаки программ-вымогателей.

Кроме того, источником угроз доступности являются непреднамеренные человеческие ошибки: случайное удаление файлов или записей в базах данных, ошибочные настройки систем; отказ в обслуживании в результате превышения допустимой мощности или недостатка ресурсов оборудования, либо аварий сетей связи; неудачно проведённое обновление аппаратного или программного обеспечения.

Существенную роль в нарушении доступности играют также природные катастрофы: землетрясения, смерчи, ураганы, пожары, наводнения. Во всех случаях конечный пользователь теряет доступ к информации, необходимой для его деятельности, возникает вынужденный простой.

Недостаточные меры безопасности увеличивают риск поражения вредоносными программами, уничтожения данных, проникновения из-вне или DoS-атак. Подобные инциденты могут сделать системы недоступными для обычных пользователей.

Реализация понятия «информационная безопасность»

Составляющие информационной безопасности:

1. Законодательная, нормативно-правовая и научная база.
2. Структура и задачи органов (подразделений), обеспечивающих безопасность ИТ.
3. Организационно-технические и режимные меры и методы (Политика информационной безопасности).
4. Программно-технические способы и средства обеспечения информационной безопасности.

Нормативные документы в области информационной безопасности

В Российской Федерации к нормативно-правовым актам в области информационной безопасности относятся:

1. Акты федерального законодательства:
2. Международные договоры РФ;
3. Конституция РФ;
4. Законы федерального уровня (включая федеральные конституционные законы, кодексы);
5. Указы Президента РФ;
6. Постановления Правительства РФ;
7. Нормативные правовые акты федеральных министерств и ведомств;
8. Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

Стандарты информационной безопасности, из которых выделяют:

1. Международные стандарты;
2. Государственные (национальные) стандарты РФ;
3. Рекомендации по стандартизации;
4. Методические указания.

Организационная защита объектов информатизации

Организационная защита – составная часть системы защиты информации, определяющая и вырабатывающая порядок и правила функционирования объектов защиты и деятельности должностных лиц в целях обеспечения защиты информации.

Организационная защита обеспечивает:

1. Организацию охраны, режима, работу с кадрами, с документами;

2. Использование технических средств безопасности и информационно-аналитическую деятельность по выявлению внутренних и внешних угроз предпринимательской деятельности.

К основным организационным мероприятиям можно отнести:

1. Организацию режима и охраны. Их цель — исключение возможности тайного проникновения на территорию и в помещения посторонних лиц;

2. Организацию работы по анализу внутренних и внешних угроз конфиденциальной информации и выработке мер по обеспечению её защиты;

3. Организацию работы по проведению систематического контроля за работой персонала с конфиденциальной информацией, порядком учёта, хранения и уничтожения документов и технических носителей.

Информационная безопасность предприятия

Информационная безопасность предприятия — это состояние защищённости корпоративных данных, при которой обеспечивается их конфиденциальность, целостность, аутентичность и доступность.

Задачи систем информационной безопасности предприятия различны:

1. Обеспечение защищённого хранения информации на носителях;
2. защита данных, передаваемых по каналам связи;
3. создание резервных копий, послеаварийное восстановление и т. д.

Информационная безопасность предприятия достигается целым комплексом организационных и технических мер, направленных на защиту корпоративных данных. Организационные меры включают документированные процедуры и правила работы с разными видами информации, IT-сервисами, средствами защиты и т. д.

Обеспечение информационной безопасности — это непрерывный процесс, включающий в себя, пять ключевых этапов:

1. Оценка стоимости
2. Разработка политики безопасности
3. Реализация политики
4. Квалифицированная подготовка специалистов
5. Аудит