Информация как ценность. Понятие об информационных угрозах.

Дисциплина: Основы информационной безопасности

Паращенко Антонина Дмитриевна

Содержание

Список иллюстраций

Список таблиц

1 Информация как ценность

Информа́ция *(от лат. informātiō «представление, понятие о чём-либо» илиinformare «придавать вид, формировать, изображать»)* — абстрактные осмысленные представления суждений о каком-либо объекте.

Информация — это *знания и сведения*, которые необходимы для ориентирования и *взаимодействия с окружающей средой*.

Информа́ция - сообщение или сигнал, совокупность данных, сведения, рассматриваемые в контексте их содержания, структурной организации, динамики (процессов создания, передачи, восприятия, использования, репрезентирования, анализа, хранения и т. п.).

Ценность информации - свойство, характеризующее *потери владельца* данной информации *при реализации определенной угрозы*, выраженные в стоимостном, временном либо ином эквиваленте.

2 Информационные угрозы, их виды, причины

2.1 Информационные угрозы

Несмотря на дорогостоящие методы, у компьютерных информационных систем есть слабые места в защите информации. Неизбежным следствием стали постоянно увеличивающиеся расходы и усилия на защиту информации. Но для того, чтобы принятые меры оказались эффективными, необходимо определить, что такое угроза безопасности информации, выявить возможные каналы утечки информации и пути несанкционированного доступа к защищаемым данным. (рис.[1])

Рис. 2.1: Классификация информационных угроз

2.2 Угрозы безопасности информации (согласно Концепции ИБ ФНС)

- угрозы нарушения конфиденциальности
- угрозы нарушения целостности информации
- угрозы нарушения доступности информации

Утечка конфиденциальной информации - бесконтрольный выход конфиденциальной информации за пределы круга лиц, которым она была доверена по службе или стала известна в процессе работы

Концепция ИБ ФНС - Концепция информационной безопасности Федеральной налоговой службы

2.3 Классификация информационных угроз по факторам возникновения

Информационные угрозы могут быть обусловлены: * *естественными факторами* (стихийные бедствия — пожар, наводнение, ураган, молния и другие причины); * *человеческими факторами*, которые подразделяются на: + *угрозы, носящие случайный, неумышленный характер.* Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации (научно-техническая, коммерческая, валютно-финансовая документация); с нецеленаправленной «утечкой умов», знаний, информации (например, в связи с миграцией населения, выездом в другие страны, для воссоединения с семьей и т.п.) Это угрозы, связанные с ошибками процесса проектирования, разработки и изготовления систем и их компонент (здания, сооружения, помещения, компьютеры, средства связи, операционные системы, прикладные пр01раммы и др.) с ошибками в работе аппаратуры из-за некачественного ее изготовления; с ошибками процесса подготовки и обработки информации (ошибки программистов и пользователей из-за недостаточной квалификации и некачественного обслуживания, ошибки операторов при подготовке, вводе и выводе данных, корректировке и обработке информации); + *угрозы, обусловленные умышленными, преднамеренными действиями людей.* Это угрозы, связанные с передачей, искажением и уничтожением научных открытий, изобретений секретов производства, новых технологий но корыстным и другим антиобщественным мотивам (документация, чертежи, описания открытий и изобретений и другие материалы); подслушиванием и передачей служебных и других научнотехнических и коммерческих разговоров; с целенаправленной «утечкой умов», знаний информации (например, в связи с получением другого гражданства по корыстным мотивам). Это угрозы, связанные с несанкционированным доступом к ресурсам автоматизированной информационной системы (внесение технических изменений в средства вычислительной техники и средства связи, подключение к средствам вычислительной техники и каналам связи,

хищение носителей информации: дискет, описаний, распечаток и др.).

Пассивные угрозы, как правило, направлены на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на их функционирование. Пассивной угрозой является, например, попытка получения информации, циркулирующей в каналах связи, посредством их прослушивания.

Активные угрозы имеют целью нарушение нормального процесса функционирования системы посредством целенаправленного воздействия на аппаратные, программные и информационные ресурсы. К активным угрозам относятся, например, разрушение или радиоэлектронное подавление линий связи, искажение сведений в базах данных либо в системной информации и т.д. Источникамиактивных угроз могут быть непосредственные действия злоумышленников, программные вирусы и т.п.

Умышленные угрозы подразделяются на: * **внутренние**, возникающие внутри управляемой организации, и внешние. Внутренние угрозы чаще всего определяются социальной напряженностью и тяжелым моральным климатом. * **внешние** угрозы могут определяться злонамеренными действиями конкурентов, экономическими условиями и другими причинами (например, стихийными бедствиями). По данным зарубежных источников, получил широкое распространение промышленный шпионаж - это наносящие ущерб владельцу коммерческой тайны, незаконный сбор, присвоение и передача сведений, составляющих коммерческую тайну, лицом, не уполномоченным на это ее владельцем.

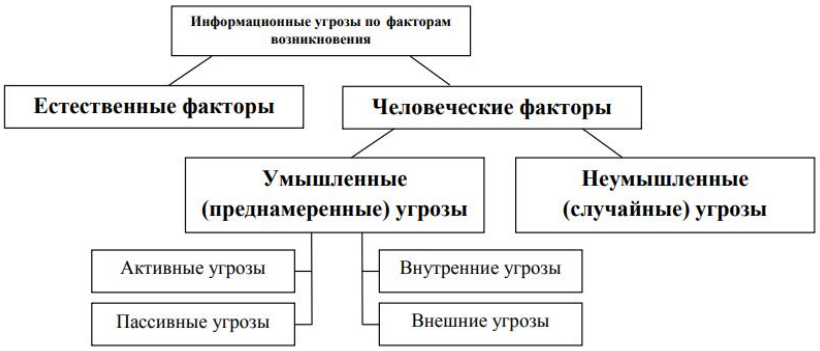

Рис. 2.2: Классификация информационных угроз по фактору возникновения

2.4 Действия и события, нарущающие информационную безопасность

Реализация угроз является следствием одного из следующих действий и событий: * разглашения конфиденциальной информации; * утечки конфиденциальной информации; * несанкционированный доступ к защищаемой информации.

Утечка конфиденциальной информации - это бесконтрольный выход конфиденциальной информации за пределы ИС или круга лиц, которым она была доверена по службе или стала известна в процессе работы. Эта утечка может быть следствием: * разглашения конфиденциальной информации; * ухода информации по различным, главным образом техническим, каналам; * несанкционированного доступа к конфиденциальной информации различными способами.

Разглашение информации ее владельцем или обладателем есть умышленные или неосторожные действия должностных лиц и пользователей, которым соответствующие сведения в установленном порядке были доверены по службе или по работе, приведшие к ознакомлению с ним лиц, не допущенных к этим сведениям.

Несанкционированный доступ (НСД) - это наиболее распространенный вид информационных угроз, который заключается в получении пользователем доступа к объекту, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности.

Рис. 2.3: Действия, нарушающие информационную безопасность

2.5 Вредоносные программы

«Троянский конь» - программа, выполняющая в дополнение к основным (проектным и документированным) не описанные в документации действия.

Вирус - это программа, которая может заражать другие программы путем включения в них своей, возможно модифицированной, копии, причем последняя сохраняет способность к дальнейшему размножению.(рис.[6]) Характеристика вирусов: * способность к саморазмножению; * высокая скорость распространения; * избирательность поражаемых систем (каждый вирус поражает только определенные системы или однородные группы систем); * наличие в большинстве случаев определенного инкубационного периода и т.д

Среда обитания	Сетевые	Распространяются по компютерной сети
	Файловые	Внедряются в выполняемые файлы
	Загрузочные	Внедряются в загрузочный сектор диска (Boot-сектор)

Рис. 2.4: Основные классы вирусов

3 Вывод

Мы узнали что такое информация, её ценность и угрозы. Понимаем классификацию угроз и как их избежать.

Список литературы

1) https://iee.unn.ru/wp-content/uploads/sites/9/2018/02/2.Inf.ugrozy-vred.programmykomp.pre
2) https://proza.ru/2020/06/17/36