ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И ЗАЩИТА ИНФОРМАЦИИ

Каналы утечки информации

Федоров Дмитрий Николаевич
dnf@dnf.su

IV

РАЗДЕЛЫ ТЕМЫ

- Основы теории информации. Коммуникационный процесс.
- Источники конфиденциальной информации и каналы ее утечки .

Раздел 1

ОСНОВЫ ТЕОРИИ ИНФОРМАЦИИ. КОММУНИКАЦИОННЫЙ ПРОЦЕСС.

ВВЕДЕНИЕ

- Чтобы дать исчерпывающую характеристику реального состояния объекта **информационной безопасности** в конкретный момент времени, необходимо описать не только сущность, виды и основы формирования угроз его информационной безопасности, но и возможные **каналы утечки конфиденциальной информации**.
- В первую очередь необходимо рассмотреть **основные понятия и некоторые основополагающие принципы теории информации**.

ТЕОРИЯ ИНФОРМАЦИИ

- Теория информации изучает количественные меры информации и способность различных систем передавать, хранить и обрабатывать информацию.
- Главная задача теории информации заключается в обнаружении математических закономерностей, управляющих системами, разработанными для связи и манипулирования информацией. Сходный круг вопросов исследует теория связи, однако она ориентирована больше на фундаментальные ограничения в области обработки и передачи информации, чем на сущность и порядок функционирования используемых средств и устройств.
- Теория информации может служить основой для изучения коммуникационного процесса с точки зрения различных проявлений негативного воздействия на передаваемую (обрабатываемую) в рамках этого процесса информацию, в особенности на информацию, подлежащую защите.
- Предлагаемые для изучения основные понятия теории информации неразрывно связаны с элементами структуры системы связи, а в некоторых случаях они сами являются этими элементами.

ПЕРЕЧЕНЬ ЭЛЕМЕНТОВ СТРУКТУРЫ СИСТЕМЫ СВЯЗИ

- **Источник информации**
- **Сообщение**
- **Отправитель сообщения**
- **Передатчик**
- **Канал распространения**
- **Приемник**
- **Получатель информации**
- **Адресат**

Далее рассмотрим подробнее указанные элементы

ЭЛЕМЕНТЫ СТРУКТУРЫ СИСТЕМЫ СВЯЗИ

- Сравнение и сопоставление элементов поможет представить систему передачи конфиденциальной информации в форме некоторого коммуникационного процесса.
- **Источник информации** — объект, осуществляющий выбор из всей совокупности информационных сообщений одного сообщения, подлежащего передаче по каналу связи адресату. В нашем случае источником информации может быть сотрудник предприятия, в установленном порядке допущенный к **конфиденциальной информации**, работающий с документами или иными ее носителями. В процессе разработки (формирования) документа осуществляется преобразование информации в форму сообщения.
- **Сообщение** — набор знаков (текст документа), с помощью которых сведения могут быть переданы другому объекту и восприняты им. В отдельных случаях в целях исключения (существенного уменьшения) вероятности овладения посторонним лицом (злоумышленником) охраняемой информацией преобразование информации в текст документа осуществляется с использованием криптографических или программно-аппаратных средств защиты.

ЭЛЕМЕНТЫ (1 ИЗ 3)

- **Отправитель сообщения** — объект, осуществляющий непосредственную передачу документа, содержащего **конфиденциальную информацию**, адресату. В роли отправителя документа может выступать сотрудник режимно-секретного подразделения (**службы безопасности**) предприятия, осуществляющий непосредственную отправку (доставку) документа по назначению (в соответствии с указанным адресом). Также отправителем может быть оператор (сотрудник структурного подразделения), осуществляющий передачу документа с использованием технических средств передачи и обработки информации (технических средств связи).
- **Передатчик** — устройство, выполняющее функцию обработки сообщения в соответствии с выбранным алгоритмом и формирования сигнала для непосредственной его передачи по каналу связи (информационному каналу).

ЭЛЕМЕНТЫ (2 ИЗ 3)

- **Канал распространения** (информационный канал или канал связи) — среда, используемая для передачи сообщения (информации) от передатчика к приемнику. Иными словами, канал представляет собой пространство между отправителем сообщения и его получателем, характеризуемое определенным расстоянием. При этом информационный канал — среда передачи сообщения в документированном (текстовом) виде, а канал связи служит для обмена информацией, представленной в речевой (звуковой, символьной и т.п.) форме. Во время передачи по каналу связи (информационному каналу) передаваемый сигнал и сообщение, содержащее **конфиденциальную информацию**, могут быть подвергнуты определенному воздействию. На сигнал воздействуют помехи, он может искажаться при передаче по каналу связи. Воздействие на сообщение может представлять собой попытки овладения содержащейся в нем информацией со стороны злоумышленника (противника, недоброжелателя, конкурента).

ЭЛЕМЕНТЫ (3 ИЗ 3)

- **Приемник** — элемент, выполняющий функцию, обратную функции передатчика. Иными словами, приемник преобразует принятый сигнал и восстанавливает по нему первоначальное сообщение. В рамках системы информационного обмена (в том числе документированной информацией) приемник можно представить в форме объекта, выполняющего также функцию доставки сообщения его получателю.
- **Получатель информации** — объект (лицо), осуществляющий фактический прием, обработку (приведение к документальному виду) и подготовку сообщения для его непосредственного доведения до сведения адресата. В роли получателя сообщения может выступить работник службы безопасности (режимно-секретного подразделения), функционально отвечающий за получение, учет, регистрацию и доведение до сведения конкретного адресата сообщения, преобразованного в форму документа.
- **Адресат** — должностное лицо (сотрудник предприятия), для которого предназначается передаваемая и принимаемая информация.

КОММУНИКАЦИОННЫЙ ПРОЦЕСС

- При выполнении элементами коммуникационного процесса своих функций возникают объективные возможности негативного воздействия со стороны злоумышленника на передаваемую и принимаемую (обрабатываемую, преобразуемую) информацию.
- Вследствие этого воздействия появляются **каналы утечки конфиденциальной информации** независимо от формы ее представления и состояния (существует ли она в форме сообщения или находится в открытом, уже преобразованном для использования виде, обработана или находится в стадии подготовки для доведения до сведения адресата и т.д.).

Раздел 2

ИСТОЧНИКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ И КАНАЛЫ ЕЕ УТЕЧКИ

ОСНОВНЫЕ ИСТОЧНИКИ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

- персонал предприятия, допущенный к конфиденциальной информации;
- носители конфиденциальной информации (документы, изделия);
- технические средства, предназначенные для хранения и обработки информации;
- средства коммуникации, используемые в целях передачи информации;
- передаваемые по каналам связи сообщения, содержащие конфиденциальную информацию.

СПОСОБЫ ОБМЕНА КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИЕЙ

Способы обмена конфиденциальной информацией (например, между сотрудниками предприятия) могут носить как:

- непосредственный (личный) характер, так и
- характер передачи формируемых на основе информации сообщений посредством технических средств и средств коммуникаций (различных средств и систем связи).

ОРГАНИЗАЦИОННЫЕ КАНАЛЫ ПЕРЕДАЧИ И ОБМЕНА ИНФОРМАЦИЕЙ

- Из существующих способов обмена **конфиденциальной информацией** необходимо выделить организационные каналы передачи и обмена информацией:
  - конфиденциальное делопроизводство (защищенный документооборот);
  - совместные работы, выполняемые предприятием по направлениям его производственной и иной деятельности;
  - совещания (конференции), в ходе которых обсуждаются вопросы конфиденциального характера;
  - рекламная и издательская (публикаторская) деятельность;
  - различные мероприятия в области сотрудничества с иностранными государствами (их представителями и организациями), связанные с обменом информацией;
  - научные исследования, деятельность диссертационных и иных советов учреждений и организаций;
  - передача сведений о деятельности предприятия и данных о его сотрудниках в территориальные инспекторские и надзорные органы.

ВОЗДЕЙСТВИЕ НА ОРГАНИЗАЦИОННЫЕ КАНАЛЫ

- Организационные каналы передачи и обмена конфиденциальной информацией в ходе их функционирования могут быть подвергнуты негативному воздействию со стороны злоумышленников, направленному на получение этой информации.
- Данное воздействие, в свою очередь, может привести к возникновению **каналов** утечки конфиденциальной информации и потребовать от руководства предприятия, руководителей структурных подразделений и персонала принятия мер по защите конфиденциальной информации, направленных на недопущение ее утечки и несанкционированного распространения (утраты носителей конфиденциальной информации).

ОПРЕДЕЛЕНИЕ МЕР ПО ЗАЩИТЕ ИНФОРМАЦИИ

- Для определения необходимых мер по защите информации нужно провести **классификацию всех возможных каналов утечки** информации в зависимости от:
  - направлений и специфики деятельности предприятия,
  - видов конфиденциальной информации,
  - особенностей функционирования системы защиты информации
  - и иных факторов.

КЛАССИФИКАЦИЯ ОРГАНИЗАЦИОННЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ (1 ИЗ 3)

Организационные каналы утечки конфиденциальной информации, возникающие в процессе деятельности предприятия, подразделяются следующим образом:

- по источникам угроз защищаемой информации (внешние и внутренние);
- по видам конфиденциальной информации или тайн (государственная, коммерческая, служебная или иная тайна; персональные данные сотрудников предприятия);
- по источникам конфиденциальной информации (персонал, носители информации, технические средства хранения и обработки информации, средства коммуникации, передаваемые или принимаемые сообщения и т.п.);
- по способам или средствам доступа к защищаемой информации (применение технических средств, непосредственная и целенаправленная работа с персоналом предприятия, осуществление непосредственного доступа к информации, получение доступа к защищаемой информации агентурным путем);

КЛАССИФИКАЦИЯ ОРГАНИЗАЦИОННЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ (2 ИЗ 3)

- по характеру взаимодействия с партнерами (каналы утечки, возникающие в отсутствие взаимодействия, при осуществлении взаимодействия, в усовиях конкурентной борьбы);
- по продолжительности или времени действия (каналы утечки постоянного, кратковременного, а также периодического или эпизодического действия);
- по направлениям деятельности предприятия (каналы утечки, возникающие в обычных условиях или при повседневной деятельности предприятия, при выполнении совместных работ, осуществлении международного сотрудничества, проведении совещаний, выезде персонала за границу, в ходе рекламной и публикаторской или издательской деятельности, при проведении научных исследований или командировании сотрудников предприятия);
- по причинам возникновения каналов утечки информации (действия злоумышленников, ошибки персонала, разглашение конфиденциальной информации, случайные обстоятельства);

КЛАССИФИКАЦИЯ ОРГАНИЗАЦИОННЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ (3 ИЗ 3)

- по каналам коммуникации, используемым для передачи, приема или обработки конфиденциальной информации (каналы утечки, возникающие при хранении, приеме-передаче, обработке или преобразовании информации, а также в канале связи, по которому передается информация);
- по месту возникновения каналов утечки информации (каналы утечки, возникающие за пределами территории предприятия или на территории предприятия — в служебных помещениях, на объектах информатизации, объектах связи и в других местах);
- по используемым способам и методам защиты информации (каналы утечки, возникающие при нарушении установленных требований по порядку отнесения информации к категории конфиденциальной, обращения с носителями информации, ограничения круга допускаемых к информации лиц, непосредственного доступа к информации персонала предприятия или командированных лиц, а также по причине нарушения требований пропускного или внутриобъектового режимов).

ИСКЛЮЧЕНИЕ ВОЗМОЖНЫХ КАНАЛОВ УТЕЧКИ ИНФОРМАЦИИ

- Задачи по исключению возможных **каналов утечки конфиденциальной информации** решаются как:
  - отдельными должностными лицами (персоналом), так и
  - структурными подразделениями предприятия, создаваемыми и функционирующими по различным направлениям защиты информации.
- Успешное решение этих задач невозможно без применения совокупности средств и методов **защиты информации**. Классификация сил, средств, способов и методов защиты информации, а также порядок их применения (использования) рассмотрены в соответствующих темах курса.

ЗАКЛЮЧЕНИЕ

- Для более полного представления о системе **защиты информации** предприятия, силах, средствах, способах, методах защиты информации, мероприятиях, планируемых и проводимых в целях обеспечения **информационной безопасности**, необходимо рассмотреть основы организационной составляющей системы защиты **конфиденциальной информации** предприятия как наиболее важного направления деятельности предприятия по защите информации.
- Это следующая тема курса.

Все материалы курса доступны для зарегистрированных пользователей Академии современных инфокоммуникационных технологий «АСИКТ»
www.acikt.ru