

## **Информационные технологии управления персоналом**

Направления подготовки: 080500.62 МЕНЕДЖМЕНТ (профиль  
Управление персоналом), 080400.62 УПРАВЛЕНИЕ ПЕРСОНАЛОМ  
Институт ИИБС, кафедра ИСПИ, ауд.1448

Винтонова Наталья Ивановна

---

# Тема 6. Концепция информационной безопасности

# Содержание

1. Понятие безопасности
2. Понятие информационной безопасности
3. Действия, приводящие к неправомерному овладению конфиденциальной информацией
4. Методы обеспечения информационной безопасности

Кто владеет информацией, тот  
владеет миром.

Натан Ротшильд

# Общее понятие "безопасность"

- широко употребляемое в русском языке, является собой "положение, при котором не угрожает опасность кому-нибудь и чему-нибудь".

# Общее понятие "безопасность"

- В.И. Даль указывал, что безопасность есть отсутствие опасности, сохранность, надежность.
- По С.И. Ожегову, безопасность - это "состояние, при котором не угрожает опасность, есть защита от опасности".

# Ст. 1 Закона о безопасности:

- Понятие безопасности – безопасность определяется как "состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз".

# Информационная безопасность

- определяется как состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государства.

# Защита информации

- - это комплекс мероприятий, направленных на обеспечение информационной безопасности.

# Информационная сфера (среда)

- - это сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации.

# Критерии информационной безопасности

Стандартная модель безопасности состоит из трех категорий:

- 1) **конфиденциальность** – доступность информации только определенному кругу лиц;
- 2) **целостность** – гарантия существования информации в исходном виде;
- 3) **доступность** – возможность получения информации авторизованным пользователем в нужное для него время.

# Существуют и другие категории модели безопасности:

- аутентичность – возможность установления автора информации;
- апеллируемость – возможность доказать, что автором является именно заявленный человек и никто другой;
- подотчётность — обеспечение идентификации субъекта доступа и регистрации его действий;
- достоверность — свойство соответствия предусмотренному поведению или результату.

# Акты федерального законодательства:

- Международные договоры РФ;
  - Конституция РФ;
  - Законы федерального уровня (включая федеральные конституционные законы, кодексы);
  - Указы Президента РФ;
  - Постановления правительства РФ;
  - Нормативные правовые акты федеральных министерств и ведомств;
  - Нормативные правовые акты субъектов РФ, органов местного самоуправления и т. д.

# К нормативно-методическим документам можно отнести:

- Методические документы государственных органов России:
  - Доктрина информационной безопасности РФ;
  - Руководящие документы ФСТЭК (Гостехкомиссии России);
  - Приказы ФСБ;

# Стандарты информационной безопасности, из которых

**выделяют:**

- Международные стандарты;
- Государственные (национальные) стандарты РФ;
- Рекомендации по стандартизации;
- Методические указания.

# Органы, обеспечивающие информационную безопасность

- Государственные органы РФ, контролирующие деятельность в области защиты информации:
  - Комитет Государственной думы по безопасности;
  - Совет безопасности России;
  - Федеральная служба по техническому и экспортному контролю (ФСТЭК);

## Государственные органы РФ, контролирующие деятельность в области защиты информации:

- Федеральная служба безопасности Российской Федерации (ФСБ России);
- Министерство внутренних дел Российской Федерации (МВД России);
- Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор).

## Службы, организующие защиту информации на уровне предприятия:

- Служба экономической безопасности;
- Служба безопасности персонала (Режимный отдел);
- Отдел кадров;
- Служба информационной безопасности.

Действия, которые могут нанести ущерб информационной безопасности организации, можно разделить на несколько категорий:

- Действия, осуществляемые авторизованными пользователями
- "Электронные" методы воздействия, осуществляемые хакерами

## Действия, осуществляемые авторизованными пользователями

- целенаправленная кража или уничтожение данных на рабочей станции или сервере;
- повреждение данных пользователем в результате неосторожных действий.

# "Электронные" методы воздействия, осуществляемые хакерами

- несанкционированное проникновение в компьютерные сети;
- DOS-атаки.

## Целью несанкционированного проникновения извне в сеть предприятия

- может быть нанесение вреда (уничтожения данных), кража конфиденциальной информации и использование ее в незаконных целях, использование сетевой инфраструктуры для организации атак на узлы третьих фирм, кража средств со счетов и т.п.

# Атака типа DOS (сокр. от Denial of Service - "отказ в обслуживании")

- - это внешняя атака на узлы сети предприятия, отвечающие за ее безопасную и эффективную работу (файловые, почтовые сервера).

# Компьютерные вирусы

- Проникновение вируса на узлы корпоративной сети может привести к нарушению их функционирования, потерям рабочего времени, утрате данных, краже конфиденциальной информации и даже прямым хищениям финансовых средств.
- Вирусная программа, проникшая в корпоративную сеть, может предоставить злоумышленникам частичный или полный контроль над деятельностью компании.

# Спам

- электронная почта в последнее время стала главным каналом распространения вредоносных программ;
- спам отнимает массу времени на просмотр и последующее удаление сообщений, вызывает у сотрудников чувство психологического дискомфорта;

# Спам

- как частные лица, так и организации становятся жертвами мошеннических схем, реализуемых спамерами;
- вместе со спамом нередко удаляется важная корреспонденция, что может привести к потере клиентов, срыву контрактов и другим неприятным последствиям.

# "Естественные" угрозы

- На информационную безопасность компании могут влиять разнообразные внешние факторы: причиной потери данных может стать неправильное хранение, кража компьютеров и носителей, форс-мажорные обстоятельства и т. д.

# Примеры естественных угроз

- пожары, наводнения, цунами, землетрясения и т.д.
- Неприятная особенность таких угроз - чрезвычайная трудность или даже невозможность их прогнозирования.
- По степени преднамеренности выделяют случайные и преднамеренные угрозы.

# Случайные угрозы

- бывают обусловлены халатностью или непреднамеренными ошибками персонала.
- В качестве примеров случайных угроз можно привести непреднамеренный ввод ошибочных данных, неумышленную порчу оборудования.

# Преднамеренные угрозы

- обычно возникают в результате направленной деятельности злоумышленника.
- Пример преднамеренной угрозы проникновение злоумышленника на охраняемую территорию с нарушением установленных правил физического доступа.

# Преднамеренные угрозы

- пассивные
- и активные.

# Пассивные угрозы

предназначены в основном на несанкционированное использование информационных ресурсов, не оказывая при этом влияния на нормальную работу самой системы.

К пассивным угрозам можно отнести несанкционированный доступ к базам данных, прослушивание каналов связи.

# Активные угрозы

- имеют цель нарушения нормальной работы системы, путем целенаправленного воздействия на ее компоненты.
- К активным угрозам можно отнести, например, вывод из строя операционной системы компьютера, разрушение ПО компьютеров, нарушение работы линий связи и т.д.

## Исторические аспекты возникновения и развития информационной безопасности

- Информационная безопасность возникла с появлением средств информационных коммуникаций между людьми, а также с осознанием человека о наличии сообществ интересов, которым может быть нанесен ущерб путём воздействия на них.

# Исторические аспекты возникновения и развития информационной безопасности

- Средства информационных коммуникаций обусловили наличие и развитие средств, которые обеспечили информационный обмен между всеми элементами социума.

## В развитии средств информационных коммуникаций можно выделить несколько этапов

- Первый этап – до 1816 года. Характеризуется он использованием естественно возникших средств информационных коммуникаций.
- В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение.

## Второй этап, начиная с 1816 года,

- связан с началом использования искусственно создаваемых технических средств электрики и радиосвязи.
- Для обеспечения скрытности и помехозащищенности радиосвязи необходимо было использовать опыт первого периода информационной безопасности на более высоком технологическом уровне.

# Третий этап – начиная с 1935 года

- связан с появлением радиолокационных и гидроакустических средств.
- Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами.

# Четвертый этап – начиная с 1946 года

- связан с изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров).
- Задачи информационной безопасности решались методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

# Пятый этап – начиная с 1965 года

- обусловлен созданием и развитием локальных информационно-коммуникационных сетей.
- Задачи информационной безопасности также решались, в основном, методами и способами физической защиты средств добывания, переработки и передачи информации, объединённых в локальную сеть путём администрирования и управления доступом к сетевым ресурсам.

# Шестой этап – начиная с 1973 года

- – связан с использованием сверхмобильных коммуникационных устройств с широким спектром задач. Угрозы информационной безопасности стали гораздо серьезнее.
- Для обеспечения информационной безопасности в компьютерных системах с беспроводными сетями передачи данных потребовалась разработка новых критериев безопасности.

# Седьмой этап, начиная с 1985 года

- связан с созданием и развитием глобальных информационно-коммуникационных сетей, с использованием космических средств обеспечения.

# Методы обеспечения информационной безопасности

- средства идентификации и аутентификации пользователей (так называемый комплекс ЗА);
- средства шифрования информации, хранящейся на компьютерах и передаваемой по сетям;
- межсетевые экраны;

# Методы обеспечения информационной безопасности

- виртуальные частные сети;
- средства контентной фильтрации;
- инструменты проверки целостности содержимого дисков;
- средства антивирусной защиты;
- системы обнаружения уязвимостей сетей и анализаторы сетевых атак.

# Комплекс ЗА"

- включает аутентификацию (или идентификацию), авторизацию и администрирование.

# Авторизация

- выполняется программой и включает в себя:
  - идентификацию и
  - аутентификацию

# Аутентификация

- - проверка подлинности, то есть того, что предъявленный идентификатор действительно принадлежит субъекту доступа.
- Выполняется на основе сопоставления имени пользователя и пароля. После аутентификации субъекту разрешается доступ к ресурсам системы на основе разрешенных ему полномочий.

# Идентификация -

- предоставление идентификатора, которым может являться несекретное имя, слово, число, для регистрации пользователя в КС.
- Субъект указывает имя пользователя, предъявленный идентификатор сравнивается с перечнем идентификаторов.

# Функция идентификации

- При попытке доступа к информационным активам функция идентификации дает ответ на вопросы: «Кто вы?» и «Где вы?» – являетесь ли вы авторизованным пользователем сети.

# Авторизация

- Наиболее часто применяемыми методами авторизации являются методы, основанные на использовании паролей (секретных последовательностей символов).
- Пароль можно установить на запуск программы, отдельные действия на компьютере или в сети. Кроме паролей для подтверждения подлинности могут использоваться пластиковые карточки и смарт-карты.

# Функция авторизации

- отвечает за то, к каким ресурсам конкретный пользователь имеет доступ.

# Функция администрирования

- заключается в наделении пользователя определенными идентификационными особенностями в рамках данной сети и определении объема допустимых для него действий.

# Администрирование

- - это регистрация действий пользователя в сети, включая его попытки доступа к ресурсам.
- Основной формой регистрации является программное ведение специальных регистрационных журналов, представляющих собой файлы на внешних носителях информации.

# Системы шифрования

- позволяют минимизировать потери в случае несанкционированного доступа к данным, хранящимся на жестком диске или ином носителе, а также перехвата информации при ее пересылке по электронной почте или передаче по сетевым протоколам.

# Межсетевой экран

- представляет собой систему или комбинацию систем, образующую между двумя или более сетями защитный барьер, предохраняющий от несанкционированного попадания в сеть или выхода из нее пакетов данных.

# Брандмауэр (firewall), межсетевой экран

- — это средство, выполняющее фильтрацию входящей и исходящей информации на основе некоторой системы правил.

# Брандмауэр (firewall), межсетевой экран

- Брандмауэры, защищающие индивидуальных пользователей и небольшие сети, реализуются в виде как аппаратных средств, так и программных продуктов, устанавливаемых на ПК.

## Технологии проверки целостности содержимого жесткого диска (integrity checking)

- обнаруживать любые действия с файлами (изменение, удаление или же просто открытие);
- идентифицировать активность вирусов, несанкционированный доступ или кражу данных авторизованными пользователями.
- Контроль осуществляется на основе анализа контрольных сумм файлов (CRC-сумм).

# Фильтры спама

- значительно уменьшают непроизводительные трудозатраты, связанные с разбором спама, снижают трафик и загрузку серверов, улучшают психологический фон в коллективе и уменьшают риск вовлечения сотрудников компании в мошеннические операции.

# Резервное копирование

- Один из основных методов защиты от потери данных - резервное копирование с четким соблюдением установленных процедур (регулярность, типы носителей, методы хранения копий и т. д.).

# Современные антивирусные технологии

- позволяют выявить практически все уже известные вирусные программы через сравнение кода подозрительного файла с образцами, хранящимися в антивирусной базе.
- Защита от вирусов может быть установлена на рабочие станции, файловые и почтовые сервера, межсетевые экраны, работающие практически под любой из распространенных операционных систем (Windows, Unix и Linux, Novell) на процессорах различных типов.

# Тестовые задания

## 1-ый вариант

1. Основной средой для информационных технологий является:

- 1) база данных
- 2) информационная система
- 3) текстовый редактор
- 4) база знаний

## 2-ой вариант

1. Оргтехника предназначена для реализации:

- 1) комплексных технологий обработки и хранения информации
- 2) технологии хранения, представления и использования информации
- 3) технологии передачи данных
- 4) технологии сбора данных

# Тестовые задания

## 1-ый вариант

2. Средства и системы телеграфной связи относятся к:

- 1) компьютерной технике
- 2) коммуникационной технике
- 3) организационной технике
- 4) кибернетике

## 2-ой вариант

2. Задача, в которой известны все элементы и взаимосвязи между ними, называется:

- 1) неформализуемой
- 2) структурированной
- 3) частично структурированной
- 4) формальной

# Тестовые задания

## 1-ый вариант

3. Множительный аппарат, предназначенный для оперативного выпуска печатной продукции, где нет слишком высоких требований по качеству печати, называется

- 1) фотоаппаратом
- 2) ризографом
- 3) ксероксом
- 4) принтером

## 2-ой вариант

3. Линейная структура управления основана на использовании принципа

- 1) соподчинения
- 2) руководства подразделениями
- 3) линейности
- 4) иерархичности

---

## Использование материалов презентации

Использование данной презентации, может осуществляться только при условии соблюдения требований законов РФ об авторском праве и интеллектуальной собственности, а также с учетом требований настоящего Заявления.

Презентация является собственностью авторов. Разрешается распечатывать копию любой части презентации для личного некоммерческого использования, однако не допускается распечатывать какую-либо часть презентации с любой иной целью или по каким-либо причинам вносить изменения в любую часть презентации. Использование любой части презентации в другом произведении, как в печатной, электронной, так и иной форме, а также использование любой части презентации в другой презентации посредством ссылки или иным образом допускается только после получения письменного согласия авторов.