Защита информации фирмы «Adidas“

Введение

- Содержание:
- 1) Виды угрозы информации;
- 2) Как защитить информацию от кражи или уничтожения;
- 3) Уровни защиты информации;
- 4) Должностная инструкция и трудовой договор;
- 5) Защита на техническом уровне;
- 6) Антивирусная программа;

Виды угроз информации

- Активные угрозы имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компоненты. *К активным угрозам относятся, например*:
- 1)Вывод из строя компьютера или его операционной системы;
- 2)Искажение сведений в БиД;
- 3)Разрушение ПО компьютеров;
- 4)Нарушение работы линий связи и т.д;
- 5)Скрытие данных- стеганография;

- Среди методов шифрования существует еще 1 способ скрытия данных – стеганография, когда скрывается не только информация, но и сам факт ее передачи.
- Именно этот способ нарушает права предприятия на обеспечение целостной, конфиденциальной и достоверной информации.

- В такой способ злоумышленники поставляют вредоносные программы, которые под видом программного обеспечения исполняют совершенно другую функцию.

- Список угроз для организации:
- Сбои в работе аппаратов;
- Мошенничество;
- Искажение информации или небрежность сотрудника;
- Использование сетевых анализаторов;
- Подлог или хищение;
- Электронные и программные «закладки»;
- Использование электромагнитного излучения, радиоизлучения или акустических сигналов;
- Вибрационные сигналы

Виды угроз информации

- *Угрозы конфиденциальности* (неправомерный доступ к информации). Угроза нарушения конфиденциальности заключается в том, что информация становится известной тому, кто не располагает полномочиями доступа к ней. Она имеет место, когда получен доступ к некоторой информации ограниченного доступа, хранящейся в вычислительной системе или передаваемой от одной системы к другой. В связи с угрозой нарушения конфиденциальности, используется термин «утечка».
- *Угрозы целостности* (неправомерное изменение данных). Угрозы нарушения целостности – это угрозы, связанные с вероятностью модификации той или иной информации, хранящейся в информационной системе. Нарушение целостности может быть вызвано различными факторами – от умышленных действий персонала до выхода из строя оборудования.
- *Угрозы доступности* (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы). Нарушение доступности представляет собой создание таких условий, при которых доступ к услуге или информации будет либо заблокирован, либо возможен за время, которое не обеспечит выполнение тех или иных бизнес-целей.

Как защитить информацию от кражи или уничтожения

- Необходимость защиты предприятия от утечки информации при работе с персоналом крайне важна. Наибольшее внимание следует уделить следующим вопросам:
- 1)На работников должна быть возложена ответственность за нарушение правил защиты от утечки информации. Если какие-то из предписанных требований не выполняются сотрудниками, необходимо оперативно применить по отношению к ним предусмотренные договором меры;
- 2)На первых этапах приема сотрудников на работу необходимо проводить проверку информации о них. Здесь важно все, начиная от характеристики и заканчивая рекомендацией. Для защиты от утечки не менее важно убедиться в соответствии сведений из резюме реальному положению дел. Не стоит забывать и о кредитной истории;
- 3)Подписание соглашения, обеспечивающего защиту информации, согласно которому кандидат обязуется не разглашать конфиденциальные сведения;
- 4)Все требования по защите информации от утечки необходимо включать в договоры, которые подписывают сотрудники. Кроме того, в этой же документации нужно прописывать ответственность за соответствующие нарушения.

Уровни защиты информации

- Можно выделить три основных уровня защиты информации:
  • защита информации на уровне рабочего места пользователя;
  • защита информации на уровне подразделения предприятия;
  • защита информации на уровне предприятия.

- Информация первоначально создается на конкретном рабочем месте рядового пользователя системы предприятия. Очень часто именно там информация хранится и первично обрабатывается.
- Рабочие места чаще всего объединяются в локальную сеть для совместной работы и обмена информацией. В данном случае мы говорим о локальной сети подразделения, пользователи которой находятся друг от друга на достаточно небольших расстояниях.
- Уровни защиты информации локальной сети подразделения отличаются более сложными механизмами, чем на рабочем месте пользователя. Защита данных на различных уровнях имеет как общие, так и специальные способы защиты.
- Локальные сети подразделений часто объединены в общую сеть предприятия, которая кроме рабочих мест рядовых пользователей имеет в своем составе также серверное оборудование и специализированные устройства, которые отвечают за функционирование и защиту всей сети предприятия. Кроме того локальные сети предприятия могут быть географически удалены друг от друга.

Уровни защиты информации

- В системе безопасности существуют следующие уровни защиты информации:
- 1)Физическая защита информации;
- 2)Контроль доступа и персональная идентификация;
- 3)Применение ключей для шифрования данных;
- 4)Защита излучения кабеля;
- 5)Защита «обратный вызов».
- Для правильного построения защитных механизмов системы безопасности следует изучить не только функционирование информационных потоков внутри предприятия, но и возможности неправомерного доступа к информации извне. В зависимости от типа угрозы, применяются определенные меры по защите информации. Поэтому каждому уровню соответствует тот или иной способ защиты информации.

Должностная инструкция и трудовой договор

- Должностные инструкции используются на разных этапах привлечения сотрудника и его работы в организации:

- 1)**При подборе персонала в компанию.** Должностная инструкция содержит информацию, необходимую для проведения обоснованного отбора работников при найме, на основе оценки соответствия кандидатов на вакантные должности требованиям организации.

- 2)**При введении в должность нового сотрудника** в период его адаптации в компании. На основе должностной инструкции можно составлять трудовой договор с работником. Это позволяет быстро ознакомить сотрудника с обязанностями и правами на новом месте, ввести его в общий процесс деятельности.

- **3)При оценке сложности работ и формировании компенсационных пакетов** для работников различных категорий в компании. Должностные инструкции используются при ранжировании работ или должностей. На основе этих данных строится система материального стимулирования.
- 4)**Для оперативного управления** деятельностью сотрудников компании. Должностная инструкция — это руководство к действию для самого работника: в ней определено, каких действий от него ожидают и по каким критериям оценивают результаты труда. Участие в обсуждении должностной инструкции предоставляет работнику возможность влиять на условия, организацию, критерии оценки своего труда.

- **5)Для оценки исполнения или аттестации сотрудников.** Должностная инструкция — основа для оценки результатов трудовой деятельности работника и его соответствия занимаемой должности, для принятия кадровых решений о повышении, перемещении, увольнении, зачислении в резерв руководящих кадров, направлении на дополнительное обучение и т. п.
- 6)**Для выявления потребности в обучении.** Должностная инструкция дает ориентиры для повышения уровня профессиональной квалификации работника и принятия решения о необходимости его переподготовки.

- Права и обязанности работника. Основные права и обязанности работника определены в ст. 21 ТК РФ, согласно которой работник имеет право на:
- - заключение, изменение и расторжение трудового договора в порядке и на условиях, установленных ТК РФ, иными федеральными законами;
- - предоставление ему работы, обусловленной трудовым договором;
- - рабочее место, соответствующее государственным нормативным требованиям охраны труда и условиям, предусмотренным коллективным договором;
- - своевременную и в полном объеме выплату заработной платы в соответствии со своей квалификацией, сложностью труда, количеством и качеством выполненной работы;
- - отдых, обеспечиваемый установлением нормальной продолжительности рабочего времени, сокращенного рабочего времени для отдельных профессий и категорий работников, предоставлением еженедельных выходных дней, нерабочих праздничных дней, оплачиваемых ежегодных отпусков;
- - полную достоверную информацию об условиях труда и требованиях охраны труда на рабочем месте;
- - профессиональную подготовку, переподготовку и повышение своей квалификации в порядке, установленном ТК РФ, иными федеральными законами;
- - объединение, включая право на создание профессиональных союзов и вступление в них для защиты своих трудовых прав, свобод и законных интересов;
- - участие в управлении организацией в предусмотренных ТК РФ, иными федеральными законами и коллективным договором формах;

- ведение коллективных переговоров и заключение коллективных договоров и соглашений
- через своих представителей, а также на информацию о выполнении коллективного договора, соглашений;
- - защиту своих трудовых прав, свобод и законных интересов всеми не запрещенными законом способами;
- - разрешение индивидуальных и коллективных трудовых споров, включая право на забастовку, в порядке, установленном ТК РФ, иными федеральными законами;
- - возмещение вреда, причиненного ему в связи с исполнением трудовых обязанностей, и компенсацию морального вреда в порядке, установленном ТК РФ, иными федеральными законами;
- - обязательное социальное страхование в случаях, предусмотренных федеральными законами.
- В трудовом договоре предусматриваются обязанности работника:
- - добросовестно исполнять свои трудовые обязанности, возложенные на него трудовым договором;
- - соблюдать правила внутреннего трудового распорядка;
- - соблюдать трудовую дисциплину;
- - выполнять установленные нормы труда;
- - соблюдать требования по охране труда и обеспечению безопасности труда;
- - бережно относиться к имуществу работодателя и других работников;
- - незамедлительно сообщить работодателю либо непосредственному руководителю о возникновении ситуации, представляющей угрозу жизни и здоровью людей, сохранности имущества работодателя.

Защита на техническом уровне

- Создавая инженерно-техническую систему, предприятие вводит в действие комплекс организационных мероприятий и ряд технических мер, которые обезопасят ценную информацию. Можно выделить 3 основных задачи, над которыми работает система:

- 1) Обезопасить здание и помещение от проникновения посторонних субъектов с целью кражи, порчи или изменения сведений;

- 2) Предотвратить порчу или полное уничтожение информационных носителей от последствий природных катаклизмов и от воздействия воды при тушении пожара;

- 3) Закрыть доступ злоумышленникам ко всем техническим каналам, по которым может произойти утечка данных.

- Инженерно-техническая защита должна отвечать современным требованиям:
- Постоянство и готовность к любым угрозам; Создание разных по уровню безопасности зон;
- Всегда опережать мошенников на 1 ход, быть в курсе технологических новинок;
- Уровень защиты информации должен быть соизмерим с важностью и ценностью сведений;
- Невозможность посторонним получить доступ к секретным данным;
- Не использовать один вид защиты, объединять разные меры и запускать в действие комплекс защитных средств;
- В первую очередь охранять самую важную информацию.

- Основные виды систем технической защиты:
- Системы охранной и "тревожной" сигнализации;
- Системы видеонаблюдения ;
- Системы контроля и управления доступом ;
- Системы пожарной сигнализации ;
- Системы оповещения и управления эвакуацией (СОУЭ);
- Системы автоматического пожаротушения;
- Системы контроля обхода (Системы контроля несения службы) ;
- Системы акустического контроля;
- Системы защиты периметра ;
- Системы резервного питания ;
- Системы охранного освещения;
- Системы контроля кассовых узлов ;
- Системы антикражных ворот;

Антивирусная программа

- Dr. Web -- антивирусы этого семейства предназначены для защиты от почтовых и сетевых червей, руткитов, файловых вирусов, троянских программ, стелс-вирусов, полиморфных вирусов, бестелесных вирусов, макровирусов, вирусов, поражающих документы MS Office, скрипт-вирусов, шпионского ПО (spyware), программ-похитителей паролей, клавиатурных шпионов, программ платного дозвона, рекламного ПО (adware), потенциально опасного ПО, хакерских утилит, программ-люков, программ-шуток, вредоносных скриптов и других вредоносных объектов, а также от спама, скаминг-, фарминг-, фишинг-сообщений и технического спама.

- Характерной особенностью антивируса Dr. Web является возможность установки на зараженную машину. В процессе установки производится сканирование памяти и файлов автозагрузки, перед сканированием производится обновление вирусной базы. При этом выпуски обновлений вирусных баз производятся с периодичностью в несколько часов и менее.

Спасибо за внимание