Министерство образования Приморского края
Краевое государственное автономное профессиональное образовательное учреждение
«Лесозаводский индустриальный колледж»

Задания для самостоятельной работы
по МДК 12 Оператор электронно-вычислительных и вычислительных машин

Специальность: 09.02.07 «Информационные системы и программирование»

Преподаватель: Грановская М.В.

2020г.

Задание:

1. Изучить и законспектировать лекцию.
2. Ответить письменно на контрольные вопросы.

***(готовую работу отправить электронную почту** mr.granovskaya.87@mail.ru)

В конспекте необходимо указать тему!!!

Защита информации

Под **безопасностью информационной системы** понимается защищенность системы от случайного или преднамеренного вмешательства в нормальный процесс ее функционирования, от попыток хищения (несанкционированного получения) информации, модификации или физического разрушения ее компонентов. Иначе говоря, это способность противодействовать различным возмущающим воздействиям на информационную систему (ИС).

Под **угрозой безопасности информации** понимаются события или действия, которые могут привести к искажению, несанкционированному использованию или даже к разрушению информационных ресурсов управляемой системы, а также программных и аппаратных средств.

Сегодня можно утверждать, что рождается новая современная технология - технология защиты информации в компьютерных информационных системах и в сетях передачи данных. Реализация этой технологии требует увеличивающихся расходов и усилий. Однако все это позволяет избежать значительно превосходящих потерь и ущерба, которые могут возникнуть при реальном осуществлении угроз ИС и информационным технологиям (ИТ).

Активные угрозы имеют целью нарушение нормального функционирования ИС путем целенаправленного воздействия на ее компоненты. К активным угрозам относятся, например:

■ вывод из строя компьютера или его операционной системы;

■ искажение сведений в базах данных;

■ разрушение программного обеспечения (ПО) компьютеров;

■ нарушение работы линий связи и т. д.

Источником активных угроз могут быть действия взломщика, вредоносные программы и т. п.

Разглашение информации ее владельцем или обладателем, 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. Возможен бесконтрольный уход конфиденциальной информации по визуально-оптическим, акустическим, электромагнитным и другим каналам.

Несанкционированный доступ - это противоправное преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к охраняемым сведениям.

Разновидности угроз информации

Логические бомбы, как вытекает из названия, используются для искажения или уничтожения информации, реже с их помощью совершаются кража или мошенничество. Манипуляциями с логическими бомбами обычно занимаются чем-то недовольные служащие, собирающиеся покинуть данную организацию, но это могут быть и консультанты, служащие с определенными политическими убеждениями и т. п.

Троянский конь - программа, выполняющая в дополнение к основным действиям, т. е. запроектированным и документированным, действия, не описанные в документации.

Вирус - программа, которая может заражать другие программы путем включения в них модифицированной копии, обладающей способностью к дальнейшему размножению.

Червь - программа, распространяющаяся через сеть и не оставляющая своей копии на магнитном носителе. Червь использует механизмы поддержки сети для определения узла, который может быть заражен. Затем с помощью тех же механизмов передает свое тело или его часть на этот узел и либо активизируется, либо ждет для этого подходящих условий.

Захватчик паролей - это программы, специально предназначенные для воровства паролей. При попытке обращения пользователя к терминалу системы на экран выводится информация, необходимая для окончания сеанса работы.

Компрометация информации (один из видов информационных инфекций) реализуется, как правило, посредством несанкционированных изменений в базе данных, в результате чего ее потребитель вынужден либо отказаться от нее, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений.

Разновидности несанкционированного использования информационных ресурсов

Несанкционированное использование информационных ресурсов, с одной стороны, является последствием ее утечки и средством ее компрометации. С другой стороны, оно имеет самостоятельное значение, так как может нанести большой ущерб управляемой системе (вплоть до полного выхода ИТ из строя) или ее абонентам.

Ошибочное использование информационных ресурсов, будучи санкционированным, тем не менее, может привести к разрушению, утечке или компрометации указанных ресурсов. Данная угроза чаще всего является следствием ошибок, имеющихся в ПО ИТ.

Несанкционированный обмен информацией между абонентами может привести к получению одним из них сведений, доступ к которым ему запрещен. Последствия те же, что и при несанкционированном доступе.

Отказ от информации состоит в непризнании получателем или отправителем этой информации фактов ее получения или отправки. Это позволяет одной из сторон расторгать заключенные финансовые соглашения «техническим» путем, формально не отказываясь от них, нанося тем самым второй стороне значительный ущерб.

Нарушение информационного обслуживания - угроза, источником которой является сама ИТ. Задержка с предоставлением информационных ресурсов абоненту может привести к

тяжелым для него последствиям. Отсутствие у пользователя своевременных данных, необходимых для принятия решения, может вызвать его нерациональные действия.

Скажем несколько слов о незаконном использовании привилегий. Любая защищенная система содержит средства, используемые в чрезвычайных ситуациях, или средства, способные функционировать с нарушением существующей политики безопасности.

Под взломом системы понимают умышленное проникновение в систему, когда взломщик не имеет санкционированных параметров для входа. Способы взлома могут быть различными, и при некоторых из них происходит совпадение с ранее описанными угрозами.

Политика безопасности представляет собой набор законов, правил и практического опыта, на основе которых строятся управление, защита и распределение конфиденциальной информации.

Методы и средства построения систем информационной безопасности. Их структура

Создание систем информационной безопасности (СИБ) в ИС и ИТ основывается на следующих принципах.

Создание систем информационной безопасности (СИБ) в ИС и ИТ основывается на следующих принципах.

1. Системный подход к построению системы зашиты, означающий оптимальное сочетание взаимосвязанных организационных, программных, аппаратных, физических и других свойств, подтвержденных практикой создания отечественных и зарубежных систем защиты и применяемых на всех этапах технологического цикла обработки информации.

2. Принцип непрерывного развития системы. Этот принцип, являющийся одним из основополагающих для компьютерных информационных систем, еще более актуален для СИБ.

3. Разделение и минимизация полномочий по доступу к обрабатываемой информации и процедурам обработки, т. е. предоставление как пользователям, так и самим работникам ИС минимума строго определенных полномочий, достаточных для выполнения ими своих служебных обязанностей.

4. Полнота контроля и регистрации попыток несанкционированного доступа, т. е. необходимость точного установления идентичности каждого пользователя и протоколирования его действий для проведения возможного расследования, а

также невозможность совершения любой операции обработки информации в ИТ без ее предварительной регистрации.

5. Обеспечение надежности системы защиты, т. е. невозможность снижения уровня надежности при возникновении в системе сбоев, отказов, преднамеренных действий взломщика или непреднамеренных ошибок пользователей и обслуживающего персонала.

6. Обеспечение контроля за функционированием системы защиты, т. е. создание средств и методов контроля работоспособности механизмов защиты.

7. Обеспечение всевозможных средств борьбы с вредоносными программами.

8. Обеспечение экономической целесообразности использования системы защиты, что выражается в превышении возможного ущерба ИС и ИТ от реализации угроз над стоимостью разработки и эксплуатации СИБ.

Выделяют следующие способы защиты информации.

■ *Правовое обеспечение защиты информации.* СовокупносСовокупность законодательных актов, нормативно-правовых документов, положений, инструкций, руководств, требования которых являются обязательными в рамках сферы их деятельности в системе защиты информации.

■ *Организационное обеспечение защиты информации.* Имеется в виду, что реализация информационной безопасности осуществляется определенными структурными единицами, такими, например, как служба безопасности фирмы и ее составные структуры: режим, охрана и др.

■ *Информационное обеспечение защиты информации.* Включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование СИБ.

■ *Техническое (аппаратное) обеспечение защиты информации.* Предполагается широкое использование технических средств как для защиты информации, так и для обеспечения деятельности СИБ.

■ *Программное обеспечение защиты информации.* Имеются в виду различные информационные, учетные, статистические и расчетные программы, обеспечивающие оценку наличия и опасности различных каналов утечки и способов несанкционированного доступа к информации.

■ *Математическое обеспечение защиты информации.* Это математические методы, используемые для различных расчетов, связанных с оценкой опасности технических средств, которыми располагают злоумышленники, зон и норм необходимой защиты.

■ *Лингвистическое обеспечение защиты информации.* Совокупность специальных языковых средств общения специалистов и пользователей в сфере обеспечения информационной безопасности.

■ *Нормативно-методическое обеспечение защиты информации.* Сюда входят нормы и регламенты деятельности органов, служб, средств, реализующих функции защиты информации; различного рода методики, обеспечивающие деятельность пользователей при выполнении своей работы в условиях жестких требований соблюдения конфиденциальности.

Из средств ПО системы защиты выделяют еще программные средства, реализующие механизмы шифрования (криптографии).

Определение

Криптография - это наука об обеспечении секретности и/или аутентичности (подлинности) передаваемых сообщений.

На *физическом уровне,* представляющем среду распространения данных (кабель, оптоволокно, радиоканал, каналообразующее оборудование), обычно применяют средства шифрования или сокрытия сигнала. Они малоприменимы в коммерческих открытых сетях, так как есть более надежное шифрование.

На *канальном уровне,* ответственном за организацию взаимодействия двух смежных узлов (двухточечные звенья), могут быть использованы средства шифрования и достоверной идентификации пользователя. Однако использование и тех, и других средств на этом уровне может оказаться избыточным. Необязательно производить шифрование (или перешифрование) на каждом двухточечном звене между двумя узлами.

Сетевой уровень решает задачи распространения и маршрутизации пакетов информации по сети в целом. Этот уровень критичен в отношении реализации средств криптозащиты. Понятие «пакет» существует и на этом уровне. На более высоких уровнях есть понятие «сообщение». Сообщение может содержать контекст или формироваться на прикладном уровне, защита которого затруднена с точки зрения управления сетью.

Этапы создания систем защиты информации

Существуют 7 этапов создания систем защиты информации.

Первый этап (анализ объекта защиты) состоит в определении того, что нужно защищать:

■ определяется информация, которая нуждается в защите;

■ выделяются наиболее важные элементы (критические) защищаемой информации;

■ определяется срок жизни критической информации (время, необходимое конкуренту для реализации добытой информации);

■ выявляются ключевые элементы информации (индикаторы), отражающие характер охраняемых сведений;

■ классифицируются индикаторы по функциональным зонам предприятия (производственно-технологические процессы, система материально-технического обеспечения производства, подразделения управления).

Второй этап предусматривает выявление угроз:

■ определяется, кого может заинтересовать защищаемая информация;

■ оцениваются методы, используемые конкурентами для получения этой информации;

■ оцениваются вероятные каналы утечки информации;

■ разрабатывается система мероприятий по пресечению действий конкурента или любого взломщика.

На *третьем этапе* проводится анализ эффективности принятых и постоянно действующих подсистем обеспечения безопасности (физическая безопасность документации, надежность

персонала, безопасность используемых для передачи конфиденциальной информации линий связи и т. д.).

На *четвертом этапе* определяются необходимые меры защиты. На основании проведенных на первых трех этапах аналитических исследований вырабатываются необходимые дополнительные меры и средства по обеспечению безопасности предприятия.

На *пятом этапе* руководители фирмы (организации) рассматривают представленные предложения по всем необходимым мерам безопасности и расчеты их стоимости и эффективности.

Шестой этап состоит в реализации принятых дополнительных мер безопасности с учетом установленных приоритетов.

Седьмой этап предполагает контроль и доведение до персонала фирмы реализуемых мер безопасности.

Контрольные вопросы

1. Какие существуют виды угроз информации? Дайте понятие угрозы.
2. Охарактеризуйте способы защиты информации.
3. Каково назначение криптографических методов защиты информации? Перечислите эти методы.
4. Дайте понятия аутентификации и цифровой подписи. В чем состоит их сущность? В чем заключаются проблемы защиты информации в сетях, и каковы возможности их разрешения?
5. Раскройте особенности стратегии защиты информации с использованием системного подхода, комплексных решений и принципа интеграции в информационных технологиях.
6. Рассмотрите этапы создания систем защиты информации.