Федеральное агентство по образованию

Государственное образовательное учреждение

Высшего профессионального образования

Уральский государственный экономический университет

КОНТРОЛЬНАЯ РАБОТА

По дисциплине Информационная безопасность

Екатеринбург 2010 г.

Вопрос 1

1. Дайте определение информации и носителя информации:

информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;

носитель информации – физическое лицо, или материальный объект, в том числе физическое поле, в которых информация находит свое отображение в виде символов, образов, сигналов, технических решений и процессов.

2. Перечислите основные аспекты обеспечения информационной безопасности и дайте их определения:

- конфиденциальность информации – гарантия того, что защищаемая информация доступна только определенному кругу пользователей, установленному правами и/или правилами доступа к ней;

- целостность информации – гарантия того, что информация существует в данный момент именно в том виде, в котором ее создал или модифицировал пользователь, обладающий правами на ее изменение;

- доступность информации – гарантия того, что к информации всегда могут получить доступ пользователи, обладающие соответствующими правами доступа.

3. Раскройте историческое развитие вопросов обеспечения конфиденциальности и целостности информации:

Первоочередной целью защиты информации подавляющий период исторического развития было обеспечение конфиденциальности. Все способы решения этой задачи издавна делились на:

- скрытное хранение и передачу;

- шифрованное хранение и передачу.

Первые свидетельства о применении методов и первой и второй группы восходят практически ко временам зарождения письменности. А начиная с XVII века, при дворах всех крупных европейских держав содержались достаточно сильные криптографы. Целью их работы было обеспечение конфиденциальной (стеганографической или шифрованной) переписки чиновников двора с удаленными владениями или войсками, а также попытки прочесть аналогичные сообщения других держав, перехваченные разведчиками.

Вопросы обеспечения целостности сообщений традиционно рассматривались отдельно от вопросов конфиденциальности – заверялась обычно подлинность только открытых сообщений. Зашифрованные послания считались неподделываемыми уже из-за самого факта неизвестности правил шифра сторонним лицам.

В первую очередь, гарантом подлинности старались сделать сам носитель информации – бумагу. При отправке сообщения из центра на периферию государства могло быть достаточным даже использование хорошей качественной бумаги с какими-либо добавками, доступными только при дворе. Более универсальным способом было заверение бумаги:

- печатью на основе воска или сургуча;

- подписью.

В конце XX века общество перешло в новую, информационную стадию, выразившуюся в:

- отделении информации от носителя;

- унификации записи информации на различные носители;

- появлении специализированных устройств обработки информации.

Этот этап характеризуется выделением защиты информации в отдельное направление, появлением своего теоретического и методического аппарата.

Вопрос 2

1. Приведите примеры угроз, которые являются нарушением целостности и доступности:

Пример для целостности – подделка документов.

Пример для доступности – взлом сервера.

2. Приведите примеры непредумышленных угроз:

Например, возгорание по халатности, приведшее к пожару и в результате потери информации (документов, физических носителей и др.).

3. К какому классу месторасположения источника Вы бы отнесли распространение компьютерных вирусов по сети предприятия?

Внутреннему, т. к. компьютерный вирус распространяется в локальной сети предприятия.

Вопрос 3

1. Перечислите основные нормативные акты в области защиты государственной тайны РФ:

- Закон РФ от 21 июля 1993 г. № 5485-1 "О государственной тайне".

- Инструкция "О порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне".

2. Перечислите основные нормативные акты в области защиты коммерческой тайны РФ.

- Закон РФ от 29 июля 2004 года № 98-ФЗ "О коммерческой тайне".

3. Какие нарушения информационной безопасности караются Уголовным Кодексом РФ?

- Нарушение неприкосновенности частной жизни

- Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

- Незаконное получение и разглашение сведений, составляющих коммерческую или банковскую тайну

- Неправомерный доступ к компьютерной информации

- Создание, использование и распространение вредоносных программ для ЭВМ

- Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

Вопрос 4

1. Перечислите возможные субъекты, объекты и операции в информационных системах.

Субъектом является человек или вычислительный процесс, который наделяется определенными правами по воздействию на объекты.

Объектом является единица хранения информации (файл, каталог, запись в базе данных и т.п.) или вычислительный процесс.

Субъекты могут выполнять над объектами определенные операции:

1. над файлами, записями и каталогами:

* создание,
* чтение,
* запись,
* добавление,
* модификацию (изменение),
* копирование,
* удаление;

1. над вычислительными процессами:

* запуск,
* останов.

2. Что такое неограниченный доступ и права доступа?

В системах с неограниченным доступом любой субъект может выполнять любую операцию над любым объектом.

Основной целью любой системы ограничения доступа является введение правил, по которым определяется, какие именно операции может выполнять каждый конкретный субъект над каждым конкретным объектом – права доступа субъекта.

3. Приведите примеры классов субъектов.

Например:

* руководитель,
* рядовой сотрудник,
* системный администратор.

4. Приведите примеры классов объектов.

Например:

* правовые документы;
* бухгалтерские документы;
* бизнес-документация (планы, отчеты, деловые предложения);
* внутренние распоряжения, инструкции, нормативно-справочные материалы.

Вопрос 5

1. Приведите известные вам примеры вредоносных программ. С какими видами Вы сталкивались лично?

Троянские кони, полиморфные вирусы и неполиморфные шифрующиеся вирусы, стелс-вирусы, медленные вирусы, ретро-вирусы, составные вирусы, вооруженные вирусы, вирусы-фаги, макровирусы, а также черви. С вирусами я не сталкивался.

2. Какие способы доставки украденной информации к злоумышленнику могут использовать программные закладки?

Интернет или намеренно встраиваемые недобросовестными разработчиками.

3. Какие свойства системы могут выбраны злоумышленником в качестве признаков для активации программной закладки?

Версия операционной системы, страна, наличие или отсутствие какого-либо программного или аппаратного обеспечения.

4. Какая схема управления вредоносным кодом наиболее опасна?

Программные закладки, позволяющие выполнять удаленное управление ими.

Вопрос 6

1. Что может послужить причиной проникновения троянской программы на защищаемый компьютер?

- программная закладка недобросовестными производителями на этапе разработки;

- умышленная установка недобросовестным сотрудником, имеющим (или имевшим ранее) полномочия для работы в системе;

- неумышленный запуск рядовым сотрудником.

2. Где в операционной системе может располагаться программный код троянской программы? Как он получает управление (активируется)?

- в прикладных программах (троянская программа активна во время работы данной прикладной программы);

- в служебных невизуальных программах операционной системы – сервисах и драйверах (создается сервис с именем и описанием, напоминающими служебные, и в течение всего времени работы компьютера троянская программа может выполнять заложенные в нее злоумышленником функции);

- в динамически загружаемых библиотеках DLL (троянская программа изменяет какую-либо часто используемую библиотеку и при каждом вызове процедуры из нее может выполнять какое-либо несанкционированное действие);

- редко – в программном коде аппаратных устройств (процедура активируется в момент инициализации устройства или при выполнении определенных действий с ним).

3. Каким образом злоумышленник может управлять троянской программой и что при этом он может сделать с атакованным компьютером?

Троянские программы, работающие по принципу ожидания управления чаще всего открывают на ожидание подключения какой-либо порт протокола TCP или UDP. В случае поступления пакетов на этот порт троянская программа выделяет из них команды, исполняет их и отправляет удаленной стороне результат.

Злоумышленник может сделать:

- кража часто встречающейся ценной информации (паролей доступа к коммутируемым линиям Интернет, номеров кредитных карт, ключей систем электронных платежей);

- полный лог и отправка вовне защищаемого периметра всех текстов (в т.ч. паролей), набираемых на клавиатуре компьютера.

Вопрос 7

1. Как Вы думаете, почему выгоднее выделять отдельные сети и обеспечивать защиту информации только на их периметре?

Внутри выделенной сети выполняется лишь минимум защитных действий, полагая, что подключенные внутри периметра пользователи – в подавляющем большинстве доверенные лица.

2. Что такое межсетевой шлюз?

Межсетевой шлюз – точка соприкосновения сетевых периметров между собой или с глобальной сетью.

3. Почему подмена адреса отправителя сообщения может нарушить целостность и доступность информации, но не нарушает ее конфиденциальность?

Информация может быть закодирована.

Вопрос 8

1. Назовите те функции системы обеспечения информационной безопасности Российской Федерации, которые общество могло бы выполнять самостоятельно, без вмешательства государства.

- оценка состояния информационной безопасности Российской Федерации, выявление источников внутренних и внешних угроз информационной безопасности, определение приоритетных направлений предотвращения, отражения и нейтрализации этих угроз;

- предупреждение, выявление и пресечение правонарушений, связанных с посягательствами на законные интересы граждан, общества и государства в информационной сфере, на осуществление судопроизводства по делам о преступлениях в этой области;

- осуществление международного сотрудничества в сфере обеспечения информационной безопасности, представление интересов Российской Федерации в соответствующих международных организациях.

Вопрос 9

1. Какой орган государственной власти координирует деятельность федеральных органов исполнительной власти и органов исполнительной власти субъектов Российской Федерации?

Правительство Российской Федерации

2. Какой орган государственной власти принимает нормативные акты в информационной сфере?

Федеральные органы исполнительной власти

Вопрос 10

1. В чем вы видите опасность закупки органами государственной власти импортных средств информатизации, телекоммуникации и связи?

Опасность встроенной шпионской прграммы

Вопрос 11

1. Какие потенциальные угрозы в информационной сфере несут конфликты на Северном Кавказе?

Вирусной атаки.

Вопрос 12

1. Какие законодательные предложения в информационной сфере вы считаете необходимыми сделать сегодня?

Конкретизацию правовых норм, устанавливающих ответственность за правонарушения в области обеспечения информационной безопасности. Развития национальных сетей связи.

Вопрос 13

1. В какой мере обеспечение информационной безопасности зависит от финансирования?

Высокая зависимость.

Вопрос 14

1. Нуждается ли современное демократическое государство в могущественных органах государственной безопасности, не приведет ли это к диктатуре и репрессиям?

Нуждается, т. к. люди порочны и их нужно держать в узде. Это не приведет к диктатуре и репрессиям: у нас не тоталитарный режим.

Вопрос 15

1. Приведите примеры наиболее перспективных направлений развития Российской экономики.

Развитие и защита систем и средств сбора, обработки, хранения и передачи статистической, финансовой, биржевой, налоговой, таможенной информации.

Вопрос 16

1. Представляет ли опасность для общества деятельность оппозиционных политических партий и движений? Если да, то каких?

Очевидно, нет или мне ничего об этом не известно.