УВАЖАЕМЫЕ СТУДЕНТЫ!

ВАМ НЕОБХОДИМО ВЫПОЛНИТЬ СЛЕДУЮЩЕЕ:

1. Ознакомиться с теорией и законспектировать лекцию не меньше трех листов, составить и ответить на вопросы.

2. Предоставит отчет конспекта лекции прислать в виде скриншото в течении трех дней.

3. Отправить преподавателю на почту **v.vika2014@mail.ru** и указать свою Ф.И.О, группу, и название дисциплины тел 072-17-44-9-22

Тема: Информационные технологии безопасности и защиты

Общие положения защиты информации

Практически вся современная информация готовится или может быть достаточно легко преобразована в машиночитаемую форму. Характерной особенностью такой информации является возможность посторонних лиц легко и незаметно исказить, скопировать или уничтожить её. Это обстоятельство вызывает необходимость организации безопасного функционирования данных в любых информационных системах. Такие мероприятия называют *защитой информации* или *информационной безопасностью*.

Противоправные действия с информацией не только затрагивают интересы государства, общества и личности, но оказывают негативные, а порой трагические и катастрофические воздействия на здания, помещения, личную безопасность обслуживающего персонала и пользователей информации. Подобные воздействия происходят также по причине стихийных бедствий, техногенных катастроф и террористических актов.

Проблемы информационной безопасности имеют не только местные (частные) и государственные, но и геополитические аспекты. Это комплексная

проблема, поэтому её решение рассматривается на разных уровнях: законодательном, административном, процедурном и программно-техническом.

Слово "*безопасность*" латинского происхождения – secure (securus). Затем в английском языке оно получило написание "security".

Общеизвестно, что "**безопасность**" – это отсутствие опасности; состояние деятельности, при которой с определённой вероятностью исключено причинение ущерба здоровью человека, зданиям, помещениям и материально-техническим средствам в них.

Безопасность — это состояние субъекта, или объекта, при котором отсутствует угроза нанесения им какого-либо ущерба.

Под **безопасностью информации** (Information security) или **информационной безопасностью** понимают защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, способных нанести ущерб владельцам и пользователям информации и поддерживающей её структуре.

При рассмотрении проблем, связанных с обеспечением безопасности, используют понятие "**несанкционированный доступ" –** это неправомочное обращение к информационным ресурсам с целью их использования (чтения, модификации), а также порчи или уничтожения. Данное понятие также связано с распространением разного рода компьютерных вирусов.

В свою очередь "**санкционированный доступ"** – это доступ к объектам, программам и данным пользователей, имеющих право выполнять определённые действия (чтение, копирование и др.), а также полномочия и права пользователей на использование ресурсов и услуг, определённых администратором вычислительной системы.

Защищённой считают ***информацию***, не претерпевшую незаконных изменений в процессе передачи, хранения и сохранения, не изменившую такие свойства, как достоверность, полнота и целостность данных.

Под терминами “**защита информации”** и “**информационная безопасность”** подразумевается совокупность методов, средств и мероприятий, направленных на исключение искажений, уничтожения и несанкционированного использования накапливаемых, обрабатываемых и хранимых данных.

В законе “Об информации, информатизации и защите информации” (ст. 20) определено, что ***целями защиты информации*** являются: предотвращение утечки, хищения, утраты, искажения, подделки информации; предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокировке информации.

Несанкционированные действия и методы воздействия на информацию, здания, помещения и людей

Основные виды и причины несанкционированных воздействий на информацию, здания, помещения и людей

Несанкционированные действия на информацию, здания, помещения и людей могут быть вызваны различными причинами и осуществляться с помощью различных методов воздействия. Подобные действия могут быть обусловлены стихийными бедствиями (ураганы, ливни, наводнения, пожары, взрывы и др.), техногенными катастрофами, террористическими актами и т.п. Борьба с ними обычно весьма затруднена из-за в значительной степени непредсказуемости таких воздействий.

Однако наибольший ущерб информации и информационным системам наносят неправомерные действия сотрудников и компьютерные вирусы. Американские специалисты утверждают, что до 85% случаев промышленного шпионажа ведётся силами сотрудников компании, в которой это происходит. В 2004 г. более трети финансовых потерь и потерь данных в организациях происходило по вине их собственных сотрудников. Решение этих проблем относится к компетенции администрации и службы безопасности организации. При этом рекомендуется шифровать даже внутрифирменную переписку.

Вирусы представляют широко распространённое явление, отражающееся на большинстве пользователей компьютеров, особенно работающих в сетях и с нелицензионным программным обеспечением.

Вирусы

> **Компьютерный вирус** — это специальная, способная к саморазмножению программа, обычно составляемая со злым умыслом.

Вирусы появились в результате создания самозапускающихся программ. Внешняя схожесть этих программ с биологией и медициной по характеру воздействия на программно-технические средства способствовала появлению таких терминов, как: вирус, заражение, лечение, профилактика, прививки, доктор и др. Процесс внедрения вирусом своей копии в другую программу (системную область диска и т.д.) называется *заражением*, а программа или иной объект, содержащий вирус – *заражёнными*.

Вирусы – это класс программ, незаконно проникающих в компьютеры пользователей и наносящих вред их программному обеспечению, информационным файлам и даже техническим устройствам, например, жёсткому магнитному диску. В России вирусы появляются в 1988 году. С развитием сетевых информационных технологий вирусы стали представлять угрозу огромному количеству пользователей сетевых и локальных компьютерных систем.

Вирусы проникают и в карманные персональные компьютеры (КПК) Первая троянская программа для КПК (Backdoor.WinCE.Brador.a – утилита скрытого дистанционного доступа) обнаружена в августе 2004 года. Она может добавлять, удалять файлы на КПК, а также пересылать их автору вируса.

Программа-вирус обычно состоит из уникальной последовательности команд – сигнатур (знаков) и поведений, что позволяет создавать обнаруживающие их программы-антивирусы. Некоторые вирусы не имеют

уникальных сигнатур и поведения и могут видоизменять самих себя (полиморфные).

По утверждению специалистов, заражение вирусами компьютеров составляет лишь доли процентов там, где работают, а не играют. Всё большую роль в области несанкционированных воздействий на информацию, здания, помещения, личную безопасность пользователя и обслуживающий персонал играют ошибочные (в т. ч. случайные) и преднамеренные действия людей.

Воздействия на информацию, здания, помещения, личную безопасность пользователя и обслуживающий персонал

Типичными *причинами нарушения безопасности на* объекте являются:

1) ошибки индивидов или неточные их действия;

2) неисправность и (или) отказ используемого оборудования;

3) непредсказуемые и недопустимые внешние проявления;

4) неисправность и (или) отсутствие необходимых средств защиты;

5) случайные и преднамеренные воздействия на информацию, защищаемые элементы оборудования, человека и окружающую среду.

Установлено, что ошибочные действия людей составляют 50–80% , а технических средств – 15–25% нарушений безопасности объектов и данных. Ошибочные и несанкционированные действия людей объясняются недостаточной их дисциплинированностью и подготовленностью к работе, опасной технологией и несовершенством используемой ими техники. Известно, что число связанных с человеческим фактором техногенных аварий и катастроф доходит до двух третей от общего их количества.

Отрицательное воздействие на человека оказывает не только незащищённость информации, но и стихийные бедствия, последствия техногенных влияний на природу, нарушения правил техники безопасности, террористические акты и другие события, приводящие, в первую очередь, к стрессовым ситуациям. Отрицательные информационные социально-психологические воздействия, в том числе дискомфорт, человек получает и в процессе работы с огромными массивами данных. Кроме стресса, он

становится жертвой информационных перегрузок, информационного шума и т.п.