Лекция № 1

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

доцент Власкин Дмитрий Николаевич

ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (УРОВЕНЬ БАКАЛАВРИАТА)

Выпускник, освоивший программу бакалавриата, должен обладать следующими общекультурными компетенциями:

способностью использовать основы философских знаний для формирования мировоззренческой позиции (ОК-1);

способностью использовать основы экономических знаний в различных сферах деятельности (ОК-2);

способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма (ОК-3);

способностью использовать основы правовых знаний в различных сферах деятельности (ОК-4);

способностью понимать социальную значимость своей будущей профессии, обладать высокой мотивацией к выполнению профессиональной деятельности в области обеспечения информационной безопасности и защиты интересов личности, общества и государства, соблюдать нормы профессиональной этики (ОК-5);

способностью работать в коллективе, толерантно воспринимая социальные, культурные и иные различия (ОК-6);

способностью к коммуникации в устной и письменной формах на русском и иностранном языках для решения задач межличностного и межкультурного взаимодействия, в том числе в сфере профессиональной деятельности (ОК-7);

способностью к самоорганизации и самообразованию (ОК-8);

способностью использовать методы и средства физической культуры для обеспечения полноценной социальной и профессиональной деятельности (ОК-9).

ФЕДЕРАЛЬНЫЙ ГОСУДАРСТВЕННЫЙ ОБРАЗОВАТЕЛЬНЫЙ СТАНДАРТ ВЫСШЕГО ОБРАЗОВАНИЯ ПО НАПРАВЛЕНИЮ ПОДГОТОВКИ 10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ (УРОВЕНЬ БАКАЛАВРИАТА)

Выпускник, освоивший программу бакалавриата, должен обладать следующими профессиональными компетенциями:

эксплуатационная деятельность:

способностью выполнять работы по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации (ПК-1);

способностью применять программные средства системного, прикладного и специального назначения, инструментальные средства, языки и системы программирования для решения профессиональных задач (ПК-2);

способностью администрировать подсистемы информационной безопасности объекта защиты (ПК-3);

способностью участвовать в работах по реализации политики информационной безопасности, применять комплексный подход к обеспечению информационной безопасности объекта защиты (ПК-4);

способностью принимать участие в организации и сопровождении аттестации объекта информатизации по требованиям безопасности информации (ПК-5);

способностью принимать участие в организации и проведении контрольных проверок работоспособности и эффективности применяемых программных, программно-аппаратных и технических средств защиты информации (ПК-6);

(продолжение)

проектно-технологическая деятельность:

способностью проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7);

способностью оформлять рабочую техническую документацию с учетом действующих нормативных и методических документов (ПК-8);

экспериментально-исследовательская деятельность:

способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов, составлять обзор по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности (ПК-9);

способностью проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10);

способностью проводить эксперименты по заданной методике, обработку, оценку погрешности и достоверности их результатов (ПК-11);

способностью принимать участие в проведении экспериментальных исследований системы защиты информации (ПК-12);

организационно-управленческая деятельность:

способностью принимать участие в формировании, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации (ПК-13);

способностью организовывать работу малого коллектива исполнителей в профессиональной деятельности (ПК-14);

способностью организовывать технологический процесс защиты информации ограниченного доступа в соответствии с нормативными правовыми актами и нормативными методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю (ПК-15)

Общая характеристика специальностей группы специальностей 10.03.01 «Информационная безопасность» бакалавриат

Профессии

ERP-программист (разрабатывает технические проекты производственных процессов и операций, управления персоналом, финансовыми потоками и активами, внедряет их и поддерживает работоспособность, синхронизируя работу разных отделов предприятия)

IT-специалист (разрабатывает программы и приложения, реализует программно-аппаратные идеи)

Администратор базы данных (отвечает за выработку требований к базе данных, её проектирование, реализацию, эффективное использование и сопровождение, включая управление учётными записями пользователей БД и защиту от несанкционированного доступа. Не менее важной функцией администратора БД является поддержка целостности базы данных)

Инженер по защите информации (выполняет работу по проектированию и внедрению специальных технических и программно-математических средств защиты информации, обеспечению организационных и инженерно-технических мер защиты информационных систем)

Программист (специалист, занимающийся непосредственной разработкой программного обеспечения для различного рода вычислительно-операционных систем)

Профессии (продолжение)

Разработчик баз данных (специалист по созданию и дизайну объектов базы данных SQL)

Специалист SAP (автоматизация различных бизнес-процессов и отраслевых решений, применение лучших практик и методологий внедрения комплексных информационных систем уровня ERP, техническая поддержка и сопровождение уже работающих в компании SAP-систем)

Специалист организационно-правовой защиты информации (защита персональных данных в кадровой службе, защищённый электронный документооборот, правовая защита информации, упорядочивает работы по внедрению новых технических и программных средств защиты)

Специалист по технической защите информации (работы по технической защите информации в организациях, категорированию объектов информатизации, работы по выявлению угроз безопасности информации, определению возможности технической разведки)

Специалист программно-аппаратной защиты информации (администрирование локально-вычислительной системы, обеспечивает защиту от несанкционированного доступа, устанавливает пароль и антивирусную защиту)

УЧЕБНЫЕ ВОПРОСЫ:

1. Понятие информации. Виды информации. Конфиденциальная информация
2. Классификация и анализ угроз информационной безопасности
3. Утечки информации

Первый учебный вопрос:

Понятие информации. Виды информации

Понятие информации

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ

- **Информация – сведения (сообщения, данные) независимо от формы их представления**

Категории информации

- **общедоступная информация**
- **информация ограниченного доступа**

В зависимости от порядка предоставления или распространения информация подразделяется на:

1) информацию, свободно распространяемую;
2) информацию, предоставляемую по соглашению лиц, участвующих в соответствующих отношениях;
3) информацию, которая в соответствии с федеральными законами подлежит предоставлению или распространению;
4) информацию, распространение которой в Российской Федерации ограничивается или запрещается

Законодательством Российской Федерации могут быть установлены виды информации в зависимости от ее содержания или обладателя

Виды информации

- **По способу восприятия**:

  визуальная – воспринимается органами зрения;

  аудиальная – воспринимается органами слуха;

  тактильная – воспринимается тактильными рецепторами;

  обонятельная – воспринимается обонятельными рецепторами;

  вкусовая – воспринимается вкусовыми рецепторами

- **По форме отображения**:

текстовая – что передается в виде символов, предназначенных обозначать лексемы языка;

числовая – в виде цифр и знаков, обозначающих математические действия;

графическая – в виде изображений, событий, предметов, графиков;

звуковая – устная или в виде записи передача лексем языка аудиальным путем;

мультимедиа – информация любого вида, передаваемая через компьютерные средства

- **По назначению**:

массовая – содержит тривиальные сведения и оперирует набором понятий, понятным большей части социума;

специальная – содержит специфический набор понятий, при использовании происходит передача сведений, которые могут быть не понятны основной массе социума, но необходимы и понятны в рамках узкой социальной группы, где используется данная информация;

личная – набор сведений о какой-либо личности, которые определяют социальное положение и типы социальных взаимодействий внутри популяции

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя

Информация ограниченного доступа (конфиденциальная информация) подразделяется на:

- **государственную тайну**
- **коммерческую тайну**
- **служебную тайну**
- **иную тайну (например, профессиональную тайну)**

Государственная тайна

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации

Степени секретности сведений (грифы секретности):

- ✔ особой важности
- ✔ совершенно секретно
- ✔ секретно

Перечень сведений, отнесенных к государственной тайне

(*утв. Указом Президента РФ от 30 ноября 1995 г. N 1203*)

1) сведения в военной области;
2) сведения в области экономики, науки и техники;
3) сведения в области внешней политики и экономики;
4) сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности, а также в области противодействия терроризму и в области обеспечения безопасности лиц, в отношении которых принято решение о применении мер государственной защиты

Не подлежат отнесению к государственной тайне и засекречиванию сведения:

- о чрезвычайных происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, и их последствиях, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- о состоянии экологии, здравоохранения, санитарии, демографии, образования, культуры, сельского хозяйства, а также о состоянии преступности;
- о привилегиях, компенсациях и социальных гарантиях, предоставляемых государством гражданам, должностным лицам, предприятиям, учреждениям и организациям;
- о фактах нарушения прав и свобод человека и гражданина;
- о размерах золотого запаса и государственных валютных резервах Российской Федерации;
- о состоянии здоровья высших должностных лиц Российской Федерации;
- о фактах нарушения законности органами государственной власти и их должностными лицами

Должностные лица, принявшие решения о засекречивании перечисленных сведений либо о включении их в этих целях в носители сведений, составляющих государственную тайну, ***несут уголовную, административную или дисциплинарную ответственность*** *в зависимости от причиненного обществу, государству и гражданам материального и морального ущерба*

Коммерческая тайна

Федеральный закон от 29 июля 2004 г. N 98-ФЗ
«О коммерческой тайне»
(*с изменениями и дополнениями от:*
2 февраля, 18 декабря 2006 г., 24 июля 2007 г., 11 июля 2011 г., 12 марта 2014 г., 18 апреля 2018 г.)

Коммерческая тайна – режим конфиденциальности информации, позволяющий ее обладателю при существующих или возможных обстоятельствах увеличить доходы, избежать неоправданных расходов, сохранить положение на рынке товаров, работ, услуг или получить иную коммерческую выгоду

Информация, составляющая коммерческую тайну – сведения любого характера (производственные, технические, экономические, организационные и другие), в том числе о результатах интеллектуальной деятельности в научно-технической сфере, а также сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании и в отношении которых обладателем таких сведений введен режим коммерческой тайны

Коммерческая тайна

Право на отнесение информации к информации, составляющей коммерческую тайну, и на определение перечня и состава такой информации принадлежит обладателю такой информации с учетом положений настоящего Федерального закона

Информация, составляющая коммерческую тайну, полученная от ее обладателя на основании договора или другом законном основании, считается полученной законным способом

Информация, составляющая коммерческую тайну, обладателем которой является другое лицо, считается полученной незаконно, если ее получение осуществлялось с умышленным преодолением принятых обладателем информации, составляющей коммерческую тайну, мер по охране конфиденциальности этой информации, а также если получающее эту информацию лицо знало или имело достаточные основания полагать, что эта информация составляет коммерческую тайну, обладателем которой является другое лицо, и что осуществляющее передачу этой информации лицо не имеет на передачу этой информации законного основания

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

1) содержащихся в учредительных документах юридического лица, документах, подтверждающих факт внесения записей о юридических лицах и об индивидуальных предпринимателях в соответствующие государственные реестры;
2) содержащихся в документах, дающих право на осуществление предпринимательской деятельности;
3) о составе имущества государственного или муниципального унитарного предприятия, государственного учреждения и об использовании ими средств соответствующих бюджетов;
4) о загрязнении окружающей среды, состоянии противопожарной безопасности, санитарно-эпидемиологической и радиационной обстановке, безопасности пищевых продуктов и других факторах, оказывающих негативное воздействие на обеспечение безопасного функционирования производственных объектов, безопасности каждого гражданина и безопасности населения в целом;
5) о численности, о составе работников, о системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости, и о наличии свободных рабочих мест;

Режим коммерческой тайны не может быть установлен лицами, осуществляющими предпринимательскую деятельность, в отношении следующих сведений:

(продолжение)

6) о задолженности работодателей по выплате заработной платы и социальным выплатам;

7) о нарушениях законодательства Российской Федерации и фактах привлечения к ответственности за совершение этих нарушений;

8) об условиях конкурсов или аукционов по приватизации объектов государственной или муниципальной собственности;

9) о размерах и структуре доходов некоммерческих организаций, о размерах и составе их имущества, об их расходах, о численности и об оплате труда их работников, об использовании безвозмездного труда граждан в деятельности некоммерческой организации;

10) о перечне лиц, имеющих право действовать без доверенности от имени юридического лица;

11) обязательность раскрытия которых или недопустимость ограничения доступа к которым установлена иными федеральными законами

*Должностные лица **несут ответственность** в соответствии с законодательством Российской Федерации за неправомерное отнесение сведений к коммерческой тайне, а также за не отнесение сведений к коммерческой тайне в случаях, предусмотренных законодательством Российской Федерации*

Режим «Коммерческая тайна» вступает в силу после выполнения следующих мер:

1. Определен перечень информации, составляющей коммерческую тайну;
2. Ограничен доступ к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка;
3. Организован учет лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана;
4. Урегулированы отношения по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров;
5. Нанесен на материальные носители, содержащие информацию, составляющую коммерческую тайну, или включен в состав реквизитов документов, содержащих такую информацию, гриф «Коммерческая тайна» с указанием обладателя такой информации (для юридических лиц – полное наименование и место нахождения, для индивидуальных предпринимателей – фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства)

Служебная тайна

Федеральный закон «О служебной тайне»
(Проект № 124871-4)

Служебная тайна – это охраняемая законом конфиденциальная информация о деятельности государственных органов, организаций, доступ к которой ограничен в силу служебной необходимости

Режим служебной тайны – совокупность правовых, организационных, технических и иных мер, принимаемых уполномоченными должностными лицами органов государственной власти и организаций, обеспечивающих ограничения на распространение сведений, составляющих служебную тайну, и на доступ к этим сведениям

Служебная тайна

Сведения, составляющие служебную тайну (служебная тайна) - конфиденциальные сведения, образующиеся в процессе управленческой деятельности органа или организации, распространение которых препятствует реализации органом или организацией предоставленных ему полномочий, либо иным образом отрицательно сказывается на их реализации, а также конфиденциальные сведения, полученные органом или организацией в соответствии с их компетенцией в установленном законодательством порядке

Сведения, относящиеся к служебной тайне:

Сведения, поступившие от физических и юридических лиц, других органов государственной власти и организаций, доступ к которым ограничен в соответствии с федеральными законами, при наличии на документах, содержащих эти сведения или сопроводительных документах грифа «Служебная тайна»

Не подлежат отнесению к служебной тайне сведения:

- содержащиеся в законодательных и иных правовых актах, устанавливающих права, свободы, обязанности граждан и порядок их реализации, а также правовой статус органов государственной власти, органов местного самоуправления, организаций;
- о чрезвычайных ситуациях, происшествиях и катастрофах, угрожающих безопасности и здоровью граждан, а также о стихийных бедствиях, их официальных прогнозах и последствиях;
- в области экологии, метеорологии, демографии, эпидемиологии и санитарии, культуры, сельского хозяйства, о состоянии преступности и другие сведения, необходимые для обеспечения безопасности граждан и населения в целом;
- о привилегиях, компенсациях и льготах,. предоставляемых государством гражданам, должностным лицам, организациям и учреждениям;
- о фактах нарушения прав и свобод человека и гражданина, нарушении законности должностными лицами органов государственной власти, органов местного самоуправления, организаций и учреждений;
- об использовании органами государственной власти, органами местного самоуправления бюджетных средств, иных государственных и местных ресурсов, о состоянии экономики и потребностях населения, если иное не предусмотрено федеральным законом;
- о размерах золотого запаса и государственных валютных резервах Российской Федерации;

Не подлежат отнесению к служебной тайне сведения:
(продолжение)

- о деятельности органов государственной власти и органов местного самоуправления, накапливаемые в информационных системах органов и организаций и представляющие общественный интерес или необходимые для реализации прав, свобод и обязанностей граждан, а также содержащиеся в официальных изданиях, поступающих в фонды библиотек и архивов;
- о состоянии здоровья лиц, занимающих государственные должности категории «А»;
- сведения о деятельности органов государственной власти, обязательные для размещения в информационных системах общего пользования в соответствии с законодательством Российской Федерации

Руководители органов государственной власти ***несут ответственность*** *в соответствии с законодательством Российской Федерации за неправомерное отнесение сведений к служебной тайне, а также за не отнесение сведений к служебной тайне в случаях, предусмотренных законодательством Российской Федерации*

Второй учебный вопрос:

Классификация и анализ угроз информационной безопасности

- **Угроза – потенциально возможное событие, действие, процесс или явление, которое может привести к нанесению ущерба чьим-либо интересам**
- **Угрозой информационной безопасности называется потенциально возможное событие, процесс или явление, которое посредством воздействия на информацию или компоненты АИС (автоматизированной информационной системы) может прямо или косвенно привести к нанесению ущерба интересам субъектов информационных отношений**
- **Атака – попытка реализации угрозы**
- **Нарушение – реализация угрозы**
- **Аутентичность – возможность достоверно установить автора сообщения**
- **Апеллируемость – возможность доказать, что автором является именно данный человек и никто другой**

Классификация угроз информационной безопасности:

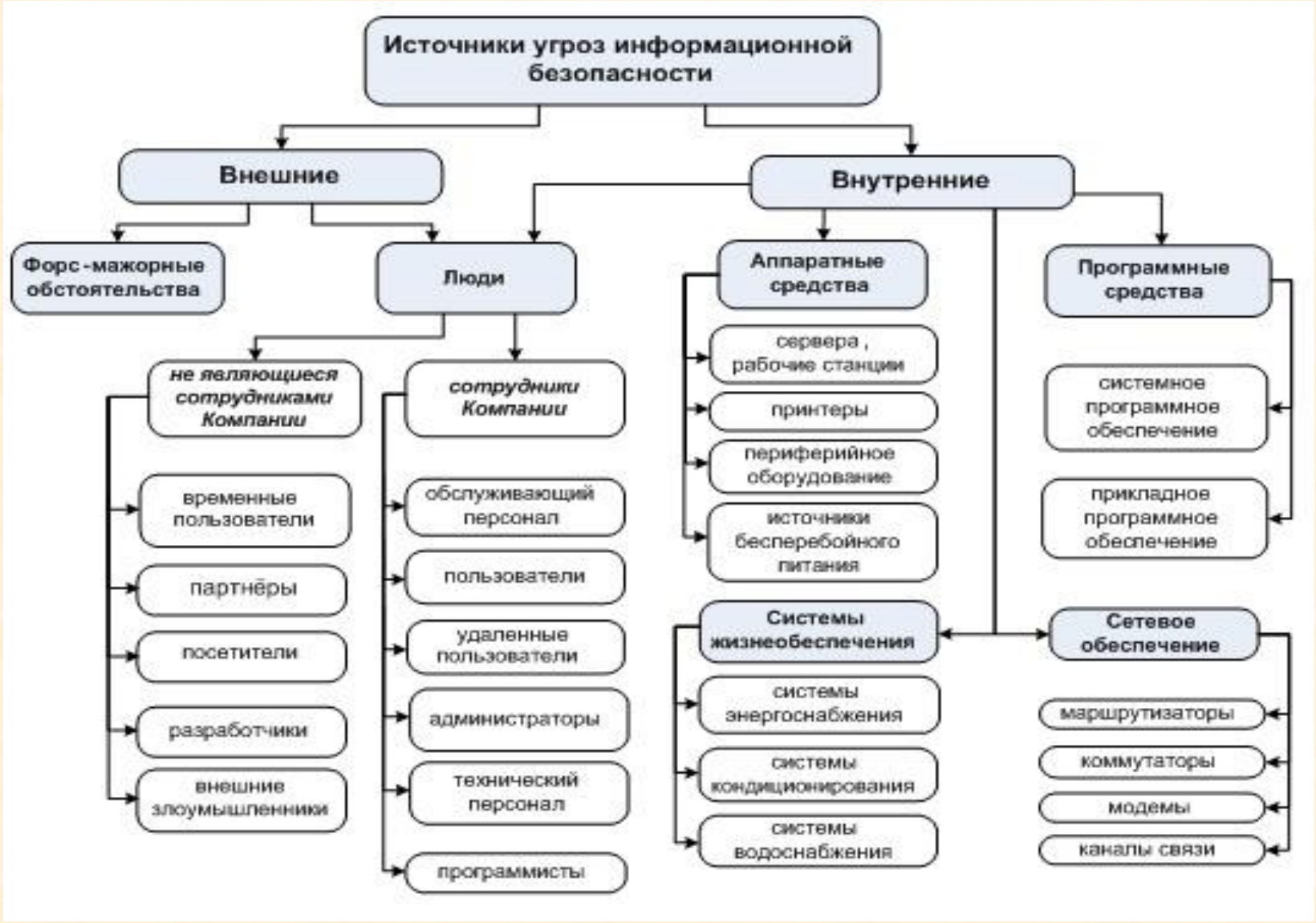
1. По аспекту ИБ: угрозы конфиденциальности, угрозы целостности, угрозы доступности. Дополнительно можно выделить угрозы аутентичности и апеллируемости

2. По компонентам АИС, на которые нацелена угроза: данные, программное обеспечение, аппаратное обеспечение, поддерживающая инфраструктура

3. По расположению источника угроз: внутри или вне рассматриваемой АИС. Угрозы со стороны инсайдеров (*лиц, имеющих доступ к скрытой и достоверной информации*) являются наиболее опасными

4. По природе возникновения: естественные (объективные) и искусственные (субъективные).

Внешние и внутренние источники угроз



Естественные угрозы – это угрозы, вызванные воздействиями на АИС и ее элементы объективных физических процессов или стихийных природных явлений, независящих от человека

Искусственные угрозы – угрозы, вызванные деятельностью человека:

непреднамеренные (неумышленные, случайные) угрозы, вызванные ошибками в проектировании АИС и ее элементов, ошибками в программном обеспечении, ошибками в действиях персонала и т.п.

преднамеренные (умышленные) угрозы, связанные с целенаправленными устремлениями злоумышленников

ОСНОВНЫЕ НЕПРЕДНАМЕРЕННЫЕ ИСКУССТВЕННЫЕ УГРОЗЫ АИС:

1. неумышленные физические действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы (неумышленная порча оборудования, удаление, искажение файлов с важной информацией или программ, в том числе системных и т.п.);
2. неправомерное отключение оборудования или изменение режимов работы устройств и программ;
3. неумышленная порча носителей информации;
4. запуск программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование носителей информации, удаление данных и т.п.);
5. нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях);
6. заражение компьютера вирусами;
7. неосторожные действия, приводящие к разглашению конфиденциальной информации, или делающие ее общедоступной;
8. разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.);
9. проектирование архитектуры системы, технологии обработки данных, разработка прикладных программ, с возможностями, представляющими опасность для работоспособности системы и безопасности информации;

ОСНОВНЫЕ НЕПРЕДНАМЕРЕННЫЕ ИСКУССТВЕННЫЕ УГРОЗЫ АС: (продолжение)

10. игнорирование организационных ограничений (установленных правил) при работе в системе;
11. вход в систему в обход средств защиты (загрузка посторонней операционной системы с внешних носителей и т.п.);
12. некомпетентное использование, настройка или неправомерное отключение средств защиты персоналом службы безопасности;
13. пересылка данных по ошибочному адресу абонента (устройства);
14. ввод ошибочных данных;
15. неумышленное повреждение каналов связи

ОСНОВНЫЕ ПРЕДНАМЕРЕННЫЕ ИСКУССТВЕННЫЕ УГРОЗЫ АИС:

1. физическое разрушение системы (путем взрыва, поджога и т.п.) или вывод из строя всех или отдельных наиболее важных компонентов компьютерной системы (устройств, носителей важной системной информации, лиц из числа персонала и т. п.);
2. отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т. п.);
3. действия по дезорганизации функционирования системы (изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных радиопомех на частотах работы устройств системы и т.п.);
4. внедрение агентов в число персонала системы (в том числе, возможно, и в административную группу, отвечающую за безопасность);
5. вербовка (путем подкупа, шантажа и т.п.) персонала или отдельных пользователей, имеющих определенные полномочия;
6. применение подслушивающих устройств, дистанционная фото- и видеосъемка и т.п.;
7. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводок активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т.п.);
8. перехват данных, передаваемых по каналам связи, и их анализ с целью выяснения протоколов обмена, правил вхождения в связь и авторизации пользователя и последующих попыток их имитации для проникновения в систему;
9. хищение носителей информации;

ОСНОВНЫЕ ПРЕДНАМЕРЕННЫЕ ИСКУССТВЕННЫЕ УГРОЗЫ АИС: (продолжение)

10. несанкционированное копирование носителей информации;
11. хищение производственных отходов (распечаток, записей, списанных носителей информации и т.п.);
12. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;
13. чтение информации из областей оперативной памяти, используемых операционной системой (в том числе подсистемой защиты) или другими пользователями, в асинхронном режиме используя недостатки операционных систем и других приложений
14. незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, путем имитации интерфейса системы и т.д.) с последующей маскировкой под зарегистрированного пользователя («маскарад»);
15. несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики, такие как номер рабочей станции в сети, физический адрес, адрес в системе связи, аппаратный блок кодирования и т.п.;
16. вскрытие шифров криптозащиты информации;
17. внедрение аппаратных спецвложений, программных «закладок» и вирусов (троянских коней), то есть таких участков программ, которые не нужны для осуществления заявленных функций, но позволяющих преодолевать систему защиты, скрытно и незаконно осуществлять доступ к системным ресурсам с целью регистрации и передачи критической информации или дезорганизации функционирования системы;

ОСНОВНЫЕ ПРЕДНАМЕРЕННЫЕ ИСКУССТВЕННЫЕ УГРОЗЫ АИС: (продолжение)

18. незаконное подключение к линиям связи с целью работы «между строк», с использованием пауз в действиях законного пользователя от его имени с последующим вводом ложных сообщений или модификацией передаваемых сообщений;
19. незаконное подключение к линиям связи с целью подмены законного пользователя путем его физического отключения после входа в систему и успешной аутентификации с последующим вводом дезинформации и навязыванием ложных сообщений

Третий учебный вопрос:

Утечки информации

КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ:

- акустическое излучение информативного речевого сигнала;
- электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям, выходящими за пределы контролируемой зоны (территория, здание, часть здания, в котором исключено неконтролируемое пребывание лиц, не имеющих постоянного или разового допуска, и посторонних транспортных средств);
- виброакустические сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации защищаемых помещений;
- несанкционированный доступ и несанкционированные действия по отношению к информации в автоматизированных системах, в том числе с использованием информационных сетей общего пользования;
- воздействие на технические или программные средства информационных систем в целях нарушения конфиденциальности, целостности и доступности информации, работоспособности технических средств, средств защиты информации посредством специально внедренных программных средств;
- хищение технических средств с хранящейся в них информацией или отдельных носителей информации;

КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ: (продолжение)

- побочные электромагнитные излучения информативного сигнала от технических средств, обрабатывающих конфиденциальную информацию, и линий передачи этой информации;
- наводки информативного сигнала, обрабатываемого техническими средствами, на цепи электропитания и линии связи, выходящие за пределы контролируемой зоны;
- радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств;
- радиоизлучения или электрические сигналы от внедренных в технические средства и защищаемые помещения специальных электронных устройств перехвата речевой информации "закладок", модулированные информативным сигналом;
- радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации;
- прослушивание ведущихся телефонных и радиопереговоров;
- просмотр информации с экранов дисплеев и других средств ее отображения, бумажных и иных носителей информации, в том числе с помощью оптических средств

Литература:

1. Невский А.Ю., Баронов О.Р. Система обеспечения информационной безопасности хозяйствующего субъекта: учебное пособие. – М.: Издательский дом МЭИ, 2009

2. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»

3. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 31 декабря 2015 г. № 583

4. Доктрина информационной безопасности Российской Федерации. Утверждена Указом Президента Российской Федерации от 5 декабря 2016 г. № 646

5. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения

Лекция № 1

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ