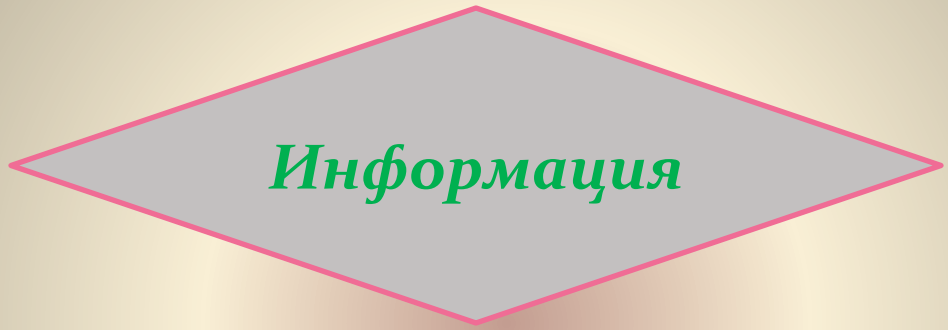
ТЕМА № 4

ИНФОРМАЦИЯ - ВАЖНЫЙ ЭЛЕМЕНТ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ

ПЛАН

1. Содержание информационной безопасности
2. Понятие и классификация угроз безопасности информации
3. Понятие и классификация информации с ограниченным доступом

1.Содержание информационной безопасности



документированные или публично объявленные сведения о событиях и явлениях, происходящих в обществе, государстве и окружающей среде

Информационная безопасность

это защищенность информационных систем и информационных ресурсов от внешних и внутренних угроз, затрудняющих эффективное использование информации обществом, государством, отдельными индивидами

Причины несовершенства отечественных систем информационной безопасности объясняются тем, что:

- информация как материальная ценность по сравнению с любой другой материальной ценностью относительно просто копируется, модернизируется или уничтожается;

- широкомасштабное развитие и внедрение вычислительной техники и телекоммуникационных систем в рамках территориально распределенной сети, переход на этой основе к безбумажной технологии, увеличение объемов и структурированности обрабатываемой информации, расширение круга ее пользователей приводит к усложнению возможности контроля и предотвращения несанкционированного получения и использование информации.

Информационная безопасность должна решать следующие задачи:

- выявление, оценка и предотвращение угроз информационным системам и информационным ресурсам;
- защита прав юридических и физических лиц на интеллектуальную собственность, а также сбор, накопление и использование информации;
- защита государственной, служебной, коммерческой и личной тайны

Выделяют следующие группы угроз информационной безопасности:

- программные - распространения вирусов, введение аппаратных и программных закладок, уничтожение и модификация сведений в информационных системах;
- технические (в том числе радиоэлектронные) - перехват информации в линиях связи;
- физические - уничтожение средств обработки и носителей информации, хищение носителей, а также аппаратных или программных парольных ключей;
- информационные - нарушение регламентов информационного обмена, незаконный сбор и использование информации, несанкционированный доступ к информационным ресурсам, незаконное кодирования данных в информационных системах, дезинформация, сокрытие или искажение информации, хищение информации из баз данных

Различают следующие мероприятия по обеспечению информационной безопасности:

- юридические;
- организационно-экономические;
- технологические

Данные меры базируются на таких принципах:

- нормативно-правовая база информационных отношений в обществе четко регламентирует механизм обеспечения права граждан свободно искать, получать, производить и распространять информацию любым законным способом;
- интересы собственников и распорядителей информационных ресурсов охраняются законом;

засекречивания (закрытие) информации является исключением из общего правила на доступ к информации;

- ответственность за сохранность информации, ее засекречивание и рассекречивание персонифицируется;

Рассматривая вопросы информационной безопасности, необходимо обратить внимание на основные направления деятельности с целью ее обеспечения:

Первый - развитие научно-практических основ информационной безопасности.

Второй - развитие законодательной и нормативно-правовой основы обеспечения информационной безопасности. Определение порядка разработки законодательных и нормативно-правовых актов, а также механизмов практической реализации принятого законодательства.

Третий - совершенствование организации форм и методов предотвращения и нейтрализации угроз информационной безопасности.

Четвертый - учитывает развитие современных методов обеспечения информационной безопасности.

2.Понятие и классификация угроз безопасности информации

информационная угроза

потенциальная возможность определенным образом нарушить информационную безопасность, или степень вероятности возникновения такого явления (события), следствием которого в могут быть нежелательные воздействия на информацию

Критерии угроз ин-й безопасности фирмы

- по аспектом информационной безопасности (доступность, целостность, конфиденциальность), на что направлены угрозы прежде;
- по компонентам информационных систем, на которые направлены угрозы (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные / преднамеренные действия природного / техногенного характера);
- по размещению источника угроз (внутри / вне информационной системы)

угрозы доступности классифицируют по компонентам информационных систем, на которые направлены угрозы:

- отказ пользователей;
- внутренняя отказ информационных систем;
- отказ поддерживающей инфраструктуры

В отношении пользователей обычно рассматриваются такие угрозы:

- нежелание работать с информационной системой (чаще всего проявляется в случае необходимости осваивать новые возможности и в случае расхождения между запросами пользователей и фактическими возможностями и техническими характеристиками)
- невозможность работать с системой из-за отсутствия соответствующей подготовки (низкий уровень общей компьютерной грамотности, неумение интерпретировать диагностические сообщения, неумение работать с документацией и т.д.)
- невозможность работать с системой из-за отсутствия технической поддержки (неполнота документации, недостаток справочной информации и т.п.)

Основными источниками внутренних отказов являются:

• отступ (случайный или преднамеренный) от установленных правил эксплуатации;

• выход системы из штатного режима эксплуатации через случайные или умышленные действия пользователей или обслуживающего персонала (превышение расчетного количества запросов, чрезмерный объем обрабатываемой информации т.п.)

• отказ программного и аппаратного обеспечения;

• облучения технических средств зондирующего сигнала, следствием чего может стать искажение или уничтожение информации, а в случае сильного облучения - выход из строя аппаратуры;

• угрозы использования специальных методов и технических средств (фотографирование, электронные закладки, уничтожающие или искажают информацию);

• уничтожение данных;

• повреждение или уничтожение аппаратуры.

Что касается поддерживающей инфраструктуры, то рекомендуется рассматривать такие угрозы:

• нарушение работы (случайное или преднамеренное) систем связи, электропитания, кондиционирования;

• повреждение или уничтожение имущества помещений;

• невозможность или нежелание обслуживающего персонала или пользователей выполнять свои обязанности (гражданские беспорядки, аварии на транспорте, террористический акт или его угроза, забастовка и т.п.)

основные типы преступных угроз информации можно классифицировать следующим образом:

• к обработке информации и без доступа злоумышленника к элементам информационной системы (подслушивание разговоров, использование оптических, визуальных или акустических средств);

• в процессе обработки информации и без доступа злоумышленника к элементам информационной системы (электромагнитные излучения; внешнее электромагнитное излучение; подключения регистрирующей аппарат туры)

• к обработке информации с доступом злоумышленника к элементам информационной системы, но без изменения последних (копирование магнитных или иных носителей, выходных или других документов)

• в процессе обработки с доступом злоумышленника к элементам информационной системы, но без изменения последних (копирование информации в процессе обработки; маскировка под зарегистрированного пользователя; программных ловушек, недостатков операционных систем и вирусов)

• к обработке информации с доступом злоумышленника к элементам информационной системы с изменением последних (подмена машинных носителей, исходящих документов, аппаратуры, элементов программ, элементов баз данных х, хищение носителей и документов; включение в программы "троянских коней", "бомб" и т.д., чтение остаточной информации после выполнения санкционированных запросов)

• в процессе обработки с доступом злоумышленника к элементам информационной системы с изменением последних;

• незаконное подключение к аппаратуре и линиям связи, снятие информации на шинах питания.

К внешним источникам угроз информации относят:

• деятельность разведывательных и специальных служб;

• деятельность политических, военных, финансовых и других экономических структур, направленная против интересов государства и бизнеса;

• преступные действия отдельных групп, формирований и физических лиц

К внутренним источникам угроз относят:

• противозаконную деятельность различных структур, группировок и отдельных лиц в сфере использования информации с целью сокрытия правонарушений, нанесение ущерба законным интересам других юридических или физических лиц.

• нарушение установленных правил сбора, обработки и передачи информации

3.Понятие и классификация информации с ограниченным доступом

- К секретной информации относится информация, содержащая сведения, составляющие государственную и другую предусмотренную законом тайну, разглашение которой наносит ущерб лицу, обществу и государству
- **Конфиденциальная информация** - это сведения, которые находятся во владении, пользовании или распоряжении отдельных физических или юридических лиц и распространяются по их желанию в соответствии с предусмотренными ими условиями

К конфиденциальной информации, являющейся собственностью государства и находится в пользовании органов государственной власти или органов местного самоуправления, предприятий, учреждений и организаций всех форм собственности, не могут быть отнесены сведения:

• о состоянии окружающей среды, качестве пищевых продуктов и предметов быта;

• об авариях, катастрофах, опасных природных явлениях и других чрезвычайных событиях, которые произошли или могут произойти и угрожают безопасности граждан;

• о состоянии здоровья населения, его жизненном уровне, включая питание, одежду, жилье, медицинское обслуживание и социальное обеспечение, а также о социально-демографических показателях, состоянии правопорядка, образования и культуры населения

• о состоянии дел с правами и свободами человека и гражданина, а также фактов их нарушений;

• о незаконных действиях органов государственной власти, органов местного самоуправления, их должностных и служебных лиц;

Сведения, относящиеся к коммерческой тайне, должны содержать следующие признаки:

• не подпадают под государственную тайну;

• не вызывают ущерб интересам общества;

• имеют действительную или потенциальную коммерческую ценность и создают преимущества в конкурентной борьбе;

• имеют ограничения в доступе, устанавливаемые руководством фирмы (предприятия);

• относительно них на фирме (предприятии) принимаются меры по их охране.

К коммерческой тайне могут быть отнесены:

• технология производства;

• технологические приемы и оборудование;

• модификация ранее известных технологий и процессов;

• результаты и программы научных исследований;

• перспективные методы управления;

• ценовая и сбытовая политика;

• сравнительные характеристики собственного ассортимента и товаров конкурентов с точки зрения качества, внешнего вида, упаковки и т.д.;

К промышленным тайнам фирмы относят основные производственные показатели, проекты, технологические инструкции, результаты проверок и испытаний, описание образцов продукции на сырье, сущность экспериментов, оценку качества процессов и изделий и т.д.

Информация о деятельности и финансового состояния предприятия, которая стала известна банку в процессе обслуживания клиента и взаимоотношений с ним или третьим лицам при предоставлении банковских услуг, и разглашение которой может нанести материальный или моральный ущерб, согласно ст. 60 Закона Украины "О банках и банковской деятельности" является **банковской тайной**

Одним из важных нормативных документов банка по безопасности является **«Положение о коммерческой тайне и конфиденциальной информации»**, которое объявляется приказом по банку. Положение предусматривает перечень сведений, что составляют коммерческую тайну и конфиденциальную информацию банка. В нем указывают, каким должностным лицам такая информация может доводиться в полном объеме, порядок ее защиты в учреждениях банка, кто отвечает за организацию мер защиты, ответственность за разглашение сведений, составляющих коммерческую тайну

Определение порядка защиты информации, организации работы с ней осуществляется согласно **«Положению об организации работы с информацией, составляющей банковскую и коммерческую тайну»** и является конфиденциальной.

Положение предусматривает: права сотрудников банка и других лиц относительно получения закрытой информации, обязанности должностных лиц и служащих банка по работе с документами, имеющими соответствующую информацию, правила ведения переговоров с помощью средств связи, общения с клиентами и посетителями

Большое внимание следует также уделить информации, которую получают посторонние лица. Существует понятие **инсайдерской информации**, то есть информации, которой владеют инсайд эры - лица, которые не работают на предприятии и, но обладают закрытой информацией об этом предприятии. Так, инсайдерами являются бывшие топ-менеджеры - лица, которые занимали руководящую должность на предприятии (начальник отдела, главный бухгалтер, заместителями к директора и т.п.), акционеры, деловые партнеры, сотрудники юридических, аудиторских и консалтинговых фирм, предоставляющих услуги вашему предприятию.