Группа ООП 3/1
Дата 20.12.2022
Вид занятия: Лекция
Тема: Основы информационной безопасности
Цель: Изучить основные угрозы и методы обеспечения информационной безопасности

План

1. Объекты информационной безопасности
2. Методы обеспечения информационной безопасности

Литература:

Основная:

1. Михеева Е.В. Информационные технологии в профессиональной деятельности: учеб. пособие для студ. сред. проф. образования. – 9-е изд., стер. – М.: Издательский центр «Академия», 2014. – 256 с.

Дополнительная:

2. Войтюшенко Н.М. Информатика и компьютерная техника: Уч. пос. баз. подготовки для студ. экон. и техн. специальностей дн. и заоч. форм обучения /Н.М.Войтюшенко, А.И.Остапец. – Донецк: ДонНУЭТ, 2014 – 485 с.

1. Объекты информационной безопасности

К объектам информационной безопасности относятся:

- все виды информационных ресурсов;
- права граждан, юридических лиц и государства на получение, распространение и использование информации, защиту информации и интеллектуальной собственности;
- система формирования, распространения и использования информационных ресурсов, включающая в себя информационные системы различного класса и назначения, библиотеки, архивы, базы и банки данных, информационные технологии и т.д.;
- информационная инфраструктура, вклбчающая центры обработки и анализа информации, каналы информационного обмена и телекоммуникации, механизмы обеспечения функционирования телекоммуникационных систем и сетей;
- система формирования общественного сознания (мировоззрение, моральные ценности, нравственные оценки, социально допустимые стереотипы поведения и взаимоотношения между людьми), базирующаяся на средствах массовой информации и пропаганды.

2. Методы обеспечения информационной безопасности

- При работе в сети Internet на первое место выходит "межсетевой экран" или брандмауэр. Брандмауэр - неотъемлемая часть системы защиты, без которой невозможна разработка ее политики. Брандмауэр позволяет значительно снизить число эффективных внешних атак на

корпоративную сеть или персональный компьютер, несанкционированный доступ к сети организации со стороны рабочих станций, удаленных и передающих серверов, включенных в сеть Internet, снизить вероятность сбора и мониторинга сетевой информации в интересах третьих лиц, блокировать доступ ненужной и вредоносной информации в систему;

- использование VPN технологии, алгоритмов криптографирования (электронной подписи, сжатия с паролем, шифрования), позволяет снизить потери от несанкционированного программно-аппаратного доступа к информации, находящейся в канале связи Internet, доступ к информации через электромагнитные излучения каналов связи и средств передачи информации Internet, также доступа к информации, размещенной на удаленных и передающих серверах Internet, сбор и мониторинг информации в интересах третьих лиц;

- дублирование канала Internet и сжатие информации позволяет повысить надежность системы в случае отказа или перегрузки канала связи и в случае стихийных бедствий;

- использование антивирусных средств, не без оснований, считается необходимым условием при подключении к Internet, позволяет значительно снизить потери информации в результате заражения вредоносными программами;

- использование автоматизированных средств проверки сети на возможные уязвимости в системе защиты и аудита безопасности корпоративных серверов позволяет установить источники угроз и значительно снизить вероятность эффективных атак на корпоративную сеть или персональный компьютер;

- использование Proxy и анонимных серверов позволяет оставаться условно анонимным при действиях в Internet и снизить риски, связанные со сбором и мониторинг сетевой информации в интересах третьих лиц, потоком ненужной и вредоносной информации в систему;

- использование систем ограничения доступа сотрудников к сетевым ресурсам Internet, использование маршрутизаторов и надежных поставщиков сетевых услуг, кратковременного канала связи позволяют сократить сбор и мониторинг сетевой информации в интересах третьих лиц, поток ненужной и вредоносной информации в систему.

Вопросы :

1. Назовите объекты информационной безопасности
2. Назовите методы обеспечения информационной безопасности
3. Какая информация считается конфедициальной

4. Что относится к национальным интересам в информационной области
5. Как проявляется информационное неравенство в системе образования

Конспект прислать по адресу
svetlana.avilova@gmail.com