СӘТБАЕВ УНИВЕРСИТЕТІ

SATBAYEV UNIVERSITY

Дисциплина «Технические средства и методы защиты информации»

Лекция 13

Организация инженерно-технической защиты информации

Преподаватель: **Батыргалиев Асхат Болатканович, PhD,**
ассоц.проф. кафедры «Кибербезопасность, обработка и хранение информации»

askhat.b.b@gmail.com

Содержание

По завершению лекции Вы будете знать:

1. Понятие инженерно-технической защиты информации
2. Классификацию средств инженерно-технической защиты информации
3. Концепцию и принципы инженерно-технической защиты информации

Понятие инженерно-технической защиты информации

Инженерно-техническая защита (ИТЗ) - комплекс мер по защите информации, включающий нормативно-правовые документы, организационные и технические меры, направленные на обеспечение безопасности информации. Основная особенность ИТЗ - это комплексность.

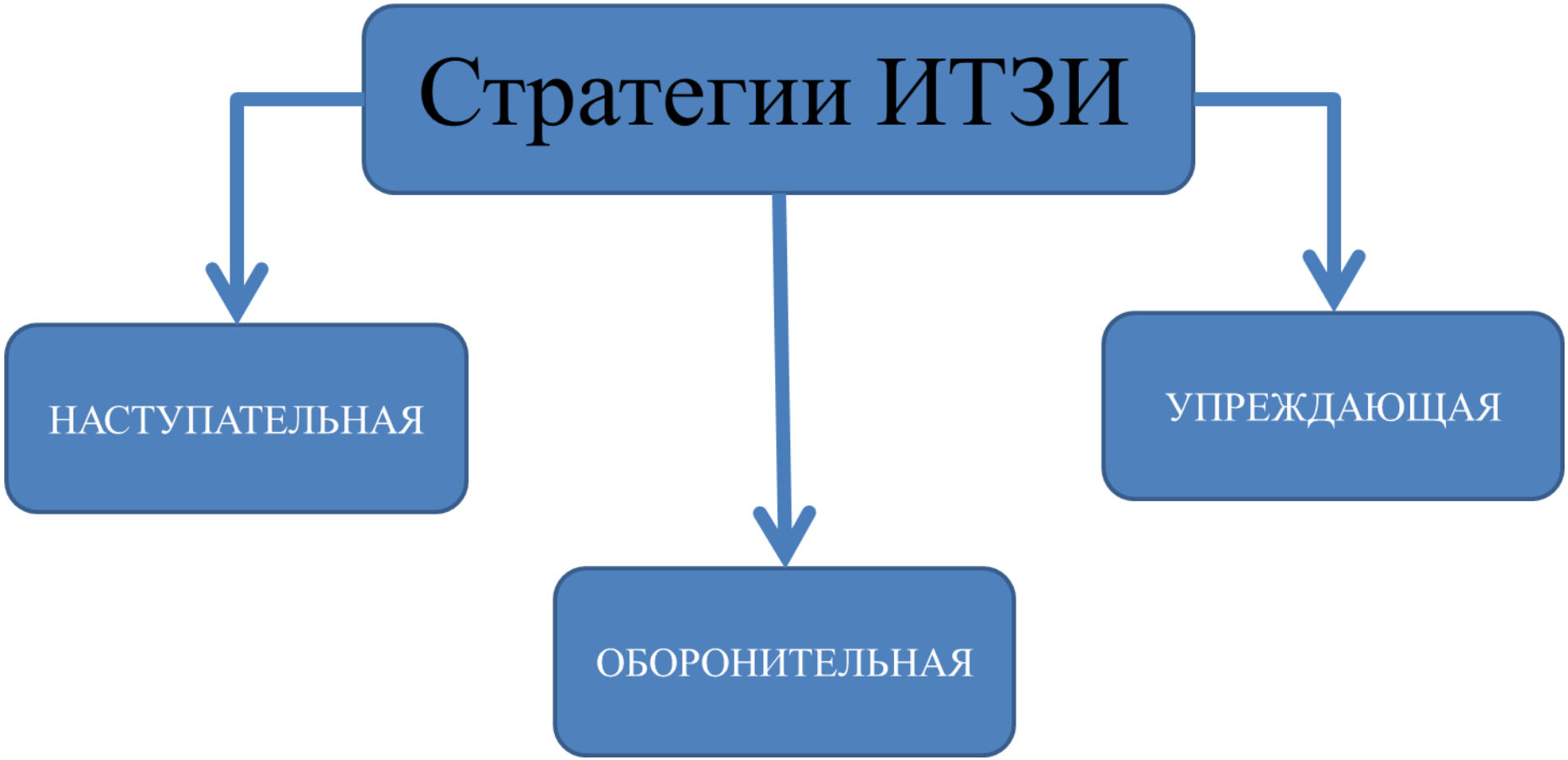
Под техническими методами ИТЗ подразумевают:

- защиту информации от несанкционированного съема техническими средствами (т.е. защита информации от утечки по техническим каналам);
- защита (охрана, физическая защита) информационных объектов.

Многообразие классификационных характеристик позволяет классифицировать инженерно-технические средства по характеристикам. ИТЗ классифицируется:

1) По объектам воздействия.
2) По характеру мероприятий.
3) По способу реализаций.
4) По масштабу охвата.
5) По классу технический средств защиты.
6) По классу средств злоумышленника.

Понятие инженерно-технической защиты информации



Классификация инженерно-технической защиты информации

По используемым средствам ИТЗ классифицируется как:

Физические - это устройства, инженерные сооружения и организационные меры, затрудняющие или исключающие проникновения злоумышленников к конфиденциальной информации. К ним относятся механические, электромеханические, электронные, электронно-оптические и радиотехнические устройства для воспрещение несанкционированного доступа проноса средств и материалов и других возможна видов преступных действий.

1) Эти средств применяются для решения задач, таких как охрана территории предприятия, зданий и внутренних помещений, а так же наблюдение за ними, охрана оборудования, продукции, финансов и информации, осуществление контролируемого доступа в здания и помещения. Охранная сигнализация и охранное телевидение например, относятся к средствам обнаружения угроз; заборы вокруг объектов - это средства предупреждения несанкционированного проникновения на территорию, а усиленные двери, стены, потолки, решетки на окнах и другие меры служат защитой и от проникновения и от других преступных действий. Средства пожаротушения относятся к системам ликвидации угроз.

Классификация инженерно-технической защиты информации

2) В общем плане по физической природе и функциональному назначению все средства этой категории можно разделить на следующие группы: **охранные и охранно-пожарные системы** (охранные системы и средства охранной сигнализации предназначены для обнаружения различных видов угроз: попыток проникновения на объект защиты, в охраняемые зоны и помещения, попыток проноса средств промышленного шпионажа, краж материальных и финансовых ценностей и других действий; оповещения сотрудников охраны или персонала объекта о появлении угроз и необходимости усиления контроля доступа на объект, территорию, в здания и помещения); **охранное телевидение** (одним из распространенных средств охраны является охранное видеонаблюдение. Привлекательной особенностью охранного видеонаблюдение является возможность не только отметить нарушение режима охраны объекта, но и контролировать обстановку вокруг него в динамике ее развития, определять опасность действий, вести скрытое наблюдение и производить видеозапись для последующего анализа правонарушения как с целью анализа, так и для привлечения к ответственности нарушителя); **охранное освещение** (обязательной составной частью системы защиты любого объекта является охранное освещение. Различают два вида охранного освещения - дежурное и тревожное. Дежурное освещение предназначается для постоянного использования в нерабочие часы, в вечернее и ночное время как на территории объекта, так и внутри здания. Тревожное освещение включается при поступлении сигнала тревоги от средства охранной сигнализации. Кроме того, по сигналу тревоги в дополнение к освещению могут включаться и звуковые приборы (звонки, сирены и пр.).

3) Также, физические средства можно разделить на три категории: средства предупреждения средства обнаружения (сигнализация) и системы ликвидации угроз.

Классификация инженерно-технической защиты информации

Аппаратные – это механические, электрические, электронные, электромеханические и др. устройства, предназначенные для защиты информации от утечки и разглашения, а также противодействия техническим средствам разведки.

Эти средства защиты информации применяются для решения следующих задач: проведения специальных исследований технических средств обеспечения на наличие каналов утечки информации;

- выявления каналов утечки информации на разных объектах;
- локализации каналов утечки информации;
- поиска и обнаружения средств шпионажа;
- противодействия несанкционированному доступу к источникам конфиденциальной информации.

По функциональному назначению аппаратные средства могут быть классифицированы на средства обнаружения средства поиска и детальных измерений, средства активного и пассивного противодействия.

В качестве примера комплекс для обнаружения и пеленгования радиозакладок, предназначенный для автоматического обнаружения и определения местонахождения радиопередатчиков, радиомикрофонов, телефонных закладок и сетевых радиопередатчиков. Это уже сложный современный поисково-обнаружительный профессиональный комплекс.

Классификация инженерно-технической защиты информации

Программные – это система спец программ, реализующих функции защиты информации и сохранения целостности и конфиденциальности.

Системы защиты компьютера от чужого вторжения классифицируются, как:

- средства собственной защиты (защита присущая самому ПО);
- средства защиты вычислительной системы (защита аппаратуры, дисков и штатных устройств);
- средства защиты с запросом информации (требуют для своей работы дополнительную информацию с целью определения полномочий пользователя);
- средства активной защиты (включаются при попытках доступа к информации без наличия на то полномочий и др. средства);
- средства пассивной защиты.

Можно выделить следующие направления использования программ для обеспечения безопасности конфиденциальной информации:

- ✓ защита информации от несанкционированного доступа;
- ✓ защита информации и программ от копирования;
- ✓ защита программ и информации от вирусов и др. зловредного ПО;
- ✓ программная защита каналов связи.

Классификация инженерно-технической защиты информации

Криптографические – это аппаратно-программные и программные средства шифрования.

Задачи криптографии является преобразование математическими методами передаваемого по каналам связи секретного сообщения, телефонного разговора или компьютерных данных таким образом, что они становится совершенно непонятными для посторонних лиц.

Основные виды криптографии: с симметричным ключом – открытым ключом№

Модель криптографической системы: вход – источник сообщения – шифрование – источник ключа – расшифрование – приемник сообщения – выход.

Комбинированные – это совокупная реализация аппаратных и программных средств, криптографических методов защиты информации.

Классификация инженерно-технической защиты информации

Классификация инженерно-технической защиты информации

Средства защиты информационных систем

Физические

Программные и аппаратные

Организационные

Психологические

Законодательные

Классификация инженерно-технической защиты информации

Средства инженерно-технической защиты обеспечивают:

- ✓ защиту территории и помещения от несанкционированного проникновения;
- ✓ защиту аппаратных средств и носителей информации;
- ✓ предотвращение возможного удаленного видеонаблюдения, подслушивания;
- ✓ предотвращение возможностей перехвата информации по техническим каналам;
- ✓ организацию доступа сотрудников в помещения;
- ✓ контроль за режимом работы персонала;
- ✓ контроль над перемещением сотрудников КС в различных производственных зонах;
- ✓ противопожарную защиту помещений;
- ✓ минимизацию материального ущерба от потерь информации из-за стихийных бедствий и техногенных аварий.

Концепция инженерно-технической защиты информации

В основу концепции защиты должны быть положены следующие принципы, аналогичные принципам добывания:

- непрерывность зашиты информации, характеризующая постоянную готовность системы защиты к отражению угроз безопасности информации в любое время;
- активность, предусматривающая прогнозирование действий злоумышленника, разработку и реализацию опережающих мер по защите;
- скрытность, исключающая ознакомление посторонних лиц со средствами и технологией защиты информации;
- целеустремленность, предполагающая сосредоточение усилий по предотвращению угроз наиболее ценной информации;
- комплексное использование различных способов и средств защиты информации, позволяющая компенсировать недостатки одних достоинствами других.

Принципы инженерно-технической защиты информации

Следующая группа принципов характеризует основные профессиональные подходы к организации защиты информации:

- соответствие уровня защиты ценности информации;
- гибкость защиты;
- многозональность защиты, предусматривающая размещение источников информации в зонах с контролируемым уровнем ее безопасности;
- многорубежность зашиты информации на пути движения злоумышленника или распространения носителя.