



КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА. ОБЗОР ПРОГРАММ ШИФРОВАНИЯ ДАННЫХ

Тема 1.3 Защищенная автоматизированная система

Введение

Что это такое?

Криптографическая защита информации предполагает использование средств шифрования данных и сложных алгоритмов кодирования.

Осуществляется с помощью программных и аппаратных (программно-аппаратных средств) средств.

Наиболее известный элемент СКЗИ – ключ с электронной подписью.

Введение

Для чего это нужно?

Защищенные таким способом электронные документы, программы практически невозможно взломать.

Следовательно, такой способ гарантирует сохранение конфиденциальных и секретных данных, предотвращает несанкционированный доступ к ним, обеспечивает безопасный обмен информацией.

Криптографическая защита

Криптография означает «тайнопись» (в переводе с греческого). Это наука, направленная на изменение данных с помощью математических способов.

Криптоанализ должен найти возможность взломать криптографическую защиту информации.

Криптология – это наука, которая объединила криптографию и криптоанализ, специализирующаяся на следующих вопросах:

- оценке надёжности системы кодирования;
- анализе стойкости кодов;
- изменении данных для защиты от запрещенных вмешательств.

Криптографическая защита

- Криптография координируется документом «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами» принятым Правительством Российской Федерации.
- Исходя из него, обязательно нужна лицензия на шифровальные средства и их техническое обслуживание.

Криптографическая защита

- Приказ ФСБ России от 9 февраля 2005 г. N 66 «Об утверждении положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (положение пкз-2005)» указывает порядок разработки и применения средств шифрования.

Классы криптографической защиты информации

К начальным классам защиты относятся КС1, КС2, КС3.

- 1. Класс КС1** присваивается, когда считается, что взлом происходит за пределами зоны, находящейся под защитой. К тому же предполагается, что атаками не будут заниматься специалисты по оценке уязвимости ПО и технических средств, а данные о системе, которую взламывают, злоумышленники берут из открытых источников.

Классы криптографической защиты информации

К начальным классам защиты относятся КС1, КС2, КС3.

- 2. Класс КС2** осуществляет такую же защиту, как и КС1, но при этом считается, что злоумышленники могут иметь доступ к защищаемой области и у них есть данные о технических методах криптографической защиты информации в информационных системах.
- 3. Класс КС3** должен противостоять таким же атакам, как и КС2, и в дополнении к этому защищать данные от лиц, которые могут иметь доступ к устройствам, установившим систему защиты.

Классы криптографической защиты информации

- 4. Класс КВ.** Данный класс способен отражать все попытки взлома КСЗ, а также намного выше сложностью, потому что производить атаки или их планировать могут разработчики или оценщики ПО и ТС, которые используются на объекте. Считается, что эти люди имели доступ к СКЗИ и могли её исследовать.
- 5. Класс КА:** отражает все угрозы КВ, но уровень безопасности выше, потому что необходимо противостоять попыткам взлома от людей, которые знают о незадекларированных способностях системного ПО и ТС защищенной системы и имеют опыт в анализе атак на аналогичные системы.

ГОСТ VPN

- ГОСТ VPN — технология, которая позволяет организовать защищенный канал связи для передачи данных в интернете. Но есть одно важное отличие от других подобных решений: здесь используется оборудование с российскими алгоритмами шифрования, сертифицированное ФСБ России.
- На практике такое решение создает зашифрованный туннель между клиентом и сервером. В нем шифрует передаваемые данные с помощью алгоритмов, одобренных ФСБ. Также решение расшифровывает входящий трафик, с этой целью оно использует специальные ключи шифрования.

ГОСТ VPN

Зачем ГОСТ VPN

- Использовать ГОСТ VPN в России необходимо многим компаниям. Такие требования содержатся в 152-ФЗ «О персональных данных», 187-ФЗ «О безопасности критической инфраструктуры РФ», положении Банка России № 672-П, ГОСТ Р 57580.1-2017, приказе Министерства энергетики № 1015, а также других законодательных и нормативных актах.

ГОСТ VPN

Зачем ГОСТ VPN

- Использовать ГОСТ VPN в России необходимо многим компаниям. Такие требования содержатся в 152-ФЗ «О персональных данных», 187-ФЗ «О безопасности критической инфраструктуры РФ», положении Банка России № 672-П, ГОСТ Р 57580.1-2017, приказе Министерства энергетики № 1015, а также других законодательных и нормативных актах.

ГОСТ VPN

В частности, решения ГОСТ VPN сегодня обязаны применять:

- банки и страховые компании,
- операторы персональных данных,
- госучреждения,
- медицинские клиники,
- предприятия, которые относятся к критической информационной инфраструктуре,
- компании, подключенные к ГосСОПКА (Государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак).

ГОСТ VPN

Применять ГОСТ VPN можно двумя способами:

- подключить программно-аппаратный комплекс on-premise,
- воспользоваться услугой сервис-провайдера.

ПАСЗИ ГОСТ VPN:

- ViPNet от «ИнфоТекс»,
- «Континент TLS VPN» от «Код Безопасности»,
- «С-Терра Шлюз» от «С-Терра СиЭсПи»,
- «Ideco МагПро ГОСТ-VPN» от Ideco.

Обзор программ шифрования данных

Что можно шифровать:

- Информацию в процессе передачи
- Информацию в процессе хранения и обработки

Обзор программ шифрования данных

Что можно шифровать:

- Информацию в процессе передачи
- Информацию в процессе хранения и обработки

Обзор программ шифрования данных

Шифрование данных в процессе хранения и обработки

- Данные шифруются средствами ОС
- Прикладное ПО для шифрования файлов или диска

ВООБРАЖЕНИЕ
КРИПТОМАНЬЯКА:

НА ЕГО НОУТЕ ВСЁ ЗАШИФРОВАНО!
ДАВАЙ ПОСТРОИМ КЛАСТЕР
ЗА МИЛЛИОН ДОЛЛАРОВ
И ВСЁ ВЗЛОМАЕМ.

НЕ ВЫЙДЕТ — ТАМ
4096-БИТНЫЙ RSA!

ЧЁРТ! НАШ
КОВАРНЫЙ
ПЛАН СОРВАН!



ЧТО ПРОИЗОШЛО БЫ
В РЕАЛЬНОСТИ:

НА ЕГО НОУТЕ ВСЁ ЗАШИФРОВАНО.
ДАЙ ЕМУ НАРКОТЫ И ДУБАСЬ
ЭТИМ ГАЕЧНЫМ КЛЮЧОМ
ЗА 5 БАКСОВ, ПОКА ОН
НЕ СКАЖЕТ ПАРОЛЬ.

ПОНЯЛ.



Обзор программ шифрования данных

Шифрование данных в процессе хранения и
обработки

- VeraCrypt
- Cryptomator
- GnuPG
- Encrypto
- 7zip
- BitLocker
- Многие другие

<https://dzen.ru/a/X74yg0ubGzMd3wJx>

Обзор программ шифрования данных

Шифрование данных в процессе передачи

- Устройства

https://www.anti-malware.ru/analytics/Market_Analysis/Russian-L2-encryption-devices-for-Ethernet-networks

- Софт

<https://openvpn.net/client/>

<https://habr.com/ru/articles/233971/>