Министерство образования Республики Беларусь
Учреждение образования
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ
Факультет Информационных Технологий и Управления
Кафедра ИТАС

Отчет по лабораторной работе №8
«Технология защиты информации»

Выполнил
студент группы
820601 Шведов А.Р

Проверил
Ярмолик В.И.

Минск, 2020

1 ЦЕЛЬ РАБОТЫ

Целью работы является изучение технологий защиты информации.

2 ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Защита информации является одним из наиболее важных и сложных аспектов информационной технологии. Специалист по информационной безопасности должен обладать глубокими специальными знаниями, регулярно отслеживать состояние в области информационной безопасности и во многом руководствоваться здравым смыслом.

Под информационной безопасностью понимают защищенность информации от случайных или преднамеренных воздействий (угроз) естественного или искусственного характера, связанных с нанесением ущерба информационной системе. Защита информации предполагает использование следующих мер и средств: физическая защита аппаратных средств, контроль действий пользователей, программная защита.

Контроль действий пользователей предполагает аутентификацию, аудит и управление рабочей средой пользователей.

Программная защита связана с анализом уязвимости программной среды, идентификацией и устранением потенциальных точек воздействия, закрытием дыр, черных ходов *(back doors)* и защитой от атак. В сети, требующей высокого уровня защиты, значительная часть работы связана с отслеживанием новых эксплойтов (документированных способов проникновения в систему) и осуществлением превентивных мер, направленных на устранение возможности их применения в сети.

Согласно *cisco* направления безопасности можно условно поделить на:

1 *Application security*
2 *Cloud security*
3 *Cryptography*
4 *Infrastructure security*
5 *Incident response*
6 *Vulnerability management*

Также выделяют 3 принципа информационной безопасности при работе с данными:

Конфиденциальность

Данные являются конфиденциальными, когда только те люди, которые имеют должны иметь на доступ к ним, могут их получить; чтобы

обеспечить конфиденциальность, вы должны быть в состоянии идентифицировать, кто пытается получить доступ к данным, и блокировать попытки тех, кто не имеет разрешения. Пароли, шифрование, аутентификация и защита от аттак–все это методы, предназначенные для обеспечения конфиденциальности.

Неприкосновенность

Поддержание данных в их правильном состоянии и предотвращение их изменений, будь то случайно или злонамеренно. Многие методы, обеспечивающие конфиденциальность, также защищают целостность данных – в конце концов, хакер не может изменить данные, к которым он не имеет доступа,но есть и другие инструменты, которые помогают обеспечить глубокую защиту целостности: контрольные суммы могут помочь вам проверить целостность данных, например, а программное обеспечение для контроля версий и частые резервные копии могут помочь вам восстановить данные в правильное состояние, если это необходимо. Целостность также охватывает концепцию неотрицания: вы должны быть в состоянии доказать, что вы сохранили целостность ваших данных, особенно в юридическом контексте.

Доступность

Антипод конфиденциальности: в то время как вы должны убедиться, что ваши данные не могут быть доступны неавторизованным пользователям, вы также должны убедиться, что они могут быть доступны тем, кто имеет соответствующие разрешения. Обеспечение доступности данных означает соответствие сетевых и вычислительных ресурсов ожидаемому объему доступа к данным и реализацию эффективной политики резервного копирования для целей аварийного восстановления.

3 ХОД РАБОТЫ

3.1 Выбор технологии шифрования на ОС Windows

3.1.1 BitLocker

Шифрование диска — технология защиты информации, переводящая данные на диске в нечитаемый код, который нелегальный пользователь не сможет легко расшифровать. Для шифрования диска используется специальное программное или аппаратное обеспечение, которое шифрует каждый бит хранилища.

BitLocker – это технология шифрования содержимого дисков компьютера, разработанная компанией *Microsoft*.

С помощью *BitLocker* можно было шифровать тома жестких дисков, но позже, уже в *Windows 7* появилась похожая технология *BitLocker To Go*, которая предназначена для шифрования съемных дисков и флешек.

3.1.2 Принцип Работы

Эта технология основывается на полном шифровании тома, выполняемом с использованием алгоритма AES (Advanced Encryption Standard). Ключи шифрования должны храниться безопасно и для этого в BitLocker есть несколько механизмов.

Самый простой, но одновременно и самый небезопасный метод — это пароль. Ключ получается из пароля каждый раз одинаковым образом, и соответственно, если кто-то узнает ваш пароль, то и ключ шифрования станет известен.

Чтобы не хранить ключ в открытом виде, его можно шифровать либо в TPM (Trusted Platform Module), либо на криптографическом токене или смарт-карте, поддерживающей алгоритм RSA 2048.

TPM — микросхема, предназначенная для реализации основных функций, связанных с обеспечением безопасности, главным образом с использованием ключей шифрования.

Модуль TPM, как правило, установлен на материнской плате компьютера, однако, приобрести в России компьютер со встроенным модулем TPM весьма затруднительно, так как ввоз устройств без нотификации ФСБ в нашу страну запрещен.

Использование смарт-карты или токена для снятия блокировки диска является одним из самых безопасных способов, позволяющих контролировать, кто выполнил данный процесс и когда. Для снятия блокировки в таком случае требуется как сама смарт-карта, так и PIN-код к ней.

Схема работы BitLocker:

1 При активации BitLocker с помощью генератора псевдослучайных чисел создается главная битовая последовательность. Это ключ шифрования тома — FVEK (full volume encryption key). Им шифруется содержимое каждого сектора. Ключ FVEK хранится в строжайшей секретности.

2 FVEK шифруется при помощи ключа VMK (volume master key). Ключ FVEK (зашифрованный ключом VMK) хранится на диске среди метаданных тома. При этом он никогда не должен попадать на диск в расшифрованном виде.

3 Сам VMK тоже шифруется. Способ его шифрования выбирает пользователь.

4 Ключ VMK по умолчанию шифруется с помощью ключа SRK (storage root key), который хранится на криптографической смарт-карте или токене. Аналогичным образом это происходит и с TPM. К слову, ключ шифрования системного диска в BitLocker нельзя защитить с помощью смарт-карты или токена. Это связано с тем, что для доступа к смарт-картам и токенам используются библиотеки от вендора, а до загрузки ОС, они, понятное дело, не доступны. Если нет TPM, то BitLocker предлагает сохранить ключ системного раздела на USB-флешке, а это, конечно, не самая лучшая идея. Если в вашей системе нет TPM, то мы не рекомендуем шифровать системные диски. И вообще шифрование системного диска является плохой идеей. При правильной настройке все важные данные хранятся отдельно от системных. Это как минимум удобнее с точки зрения их резервного копирования. Плюс шифрование системных файлов снижает производительность системы в целом, а работа незашифрованного системного диска с зашифрованными файлами происходит без потери скорости.

5 Ключи шифрования других несистемных и съемных дисков можно защитить с помощью смарт-карты или токена, а также TPM. Если ни модуля TPM ни смарт-карты нет, то вместо SRK для шифрования ключа VMK используется ключ сгенерированный на основе введенного вами пароля.

При запуске с зашифрованного загрузочного диска система опрашивает все возможные хранилища ключей — проверяет наличие TPM, проверяет USB-порты или, если необходимо, запрашивает пользователя (что называется восстановлением). Обнаружение хранилища ключа позволяет Windows расшифровать ключ VMK, которым расшифровывается ключ FVEK, уже которым расшифровываются данные на диске.

Каждый сектор тома шифруется отдельно, при этом часть ключа шифрования определяется номером этого сектора. В результате два сектора, содержащие одинаковые незашифрованные данные, будут в зашифрованном виде выглядеть по-разному, что сильно затруднит процесс определения ключей шифрования путем записи и расшифровки заранее известных данных.

Помимо FVEK, VMK и SRK, в BitLocker используется еще один тип ключей, создаваемый «на всякий случай». Это ключи восстановления.

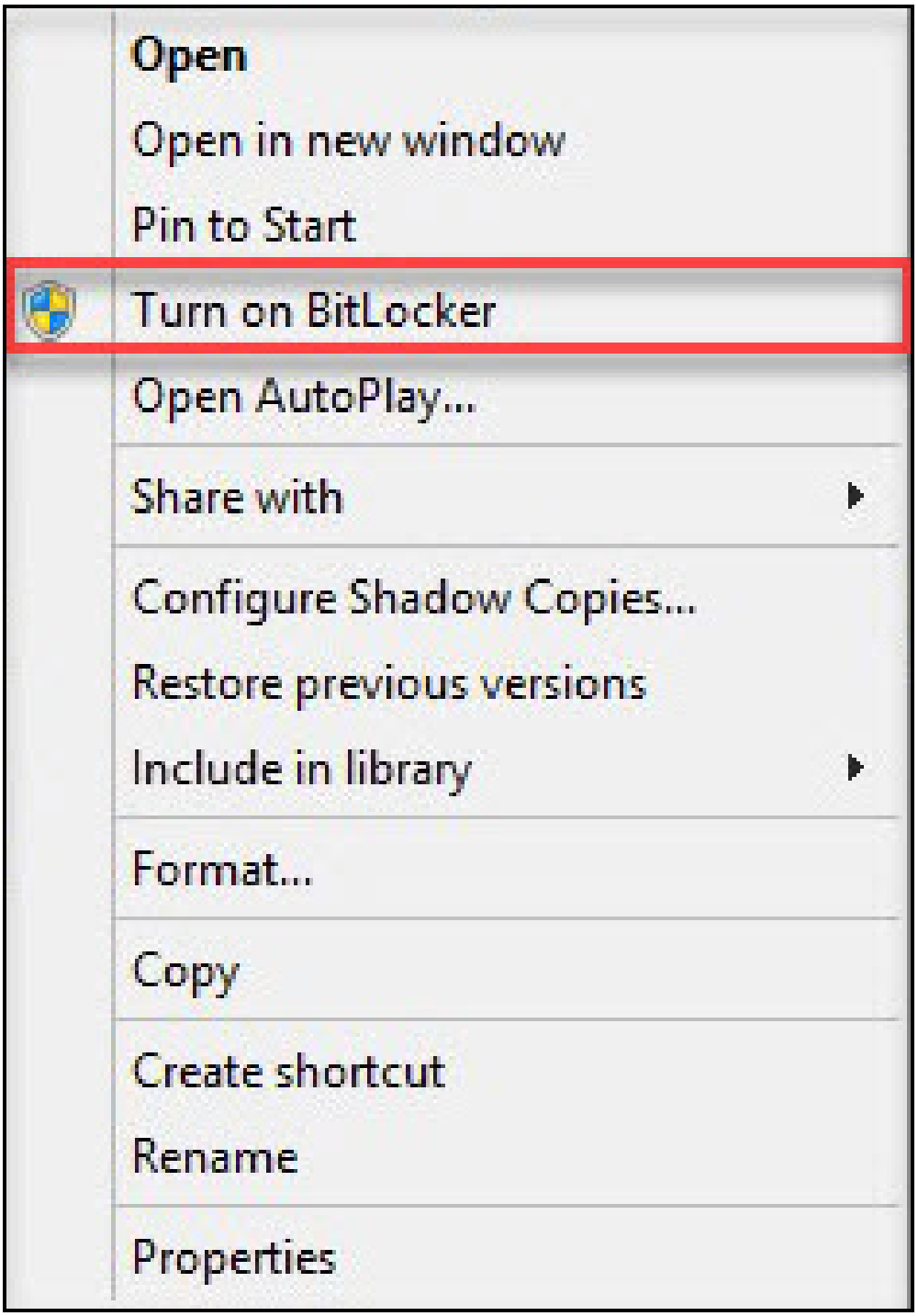
Для аварийных случаев (пользователь потерял токен, забыл его PIN-код и т.д.) BitLocker на последнем шаге предлагает создать ключ восстановления. Отказ от его создания в системе не предусмотрен.

Рисунок 3.1 – Дешифровка данных

3.1.3 Включение шифрования

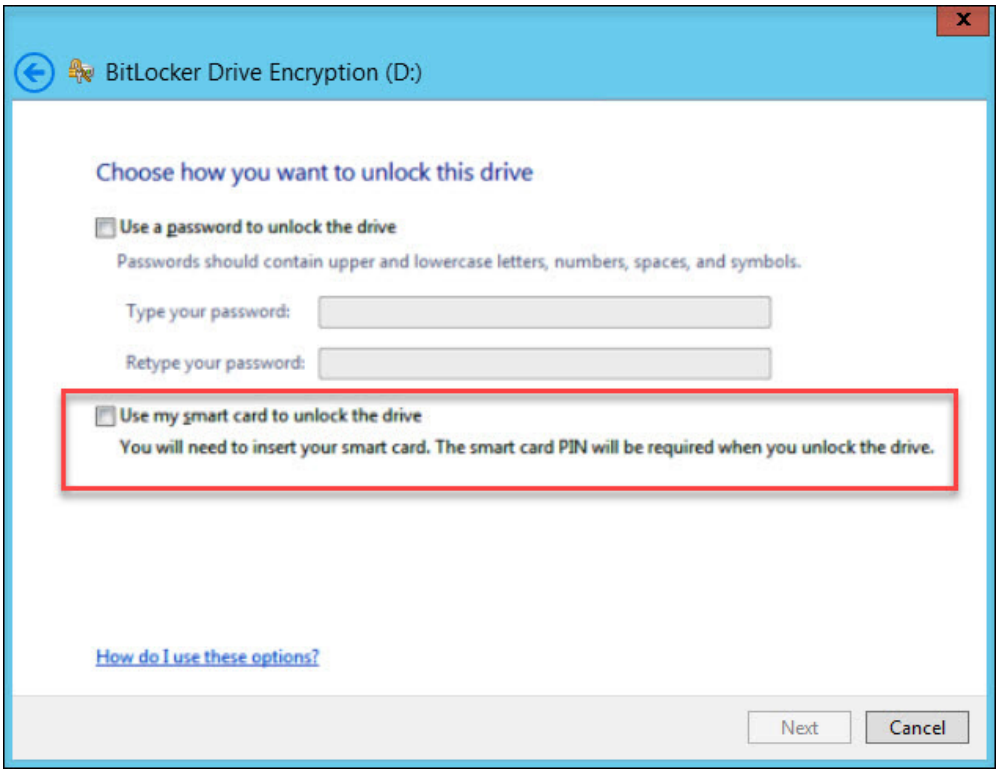
1. Вставим внешний диск и ,щелкая по названию диска, выберем пункт Turn on BitLocker.

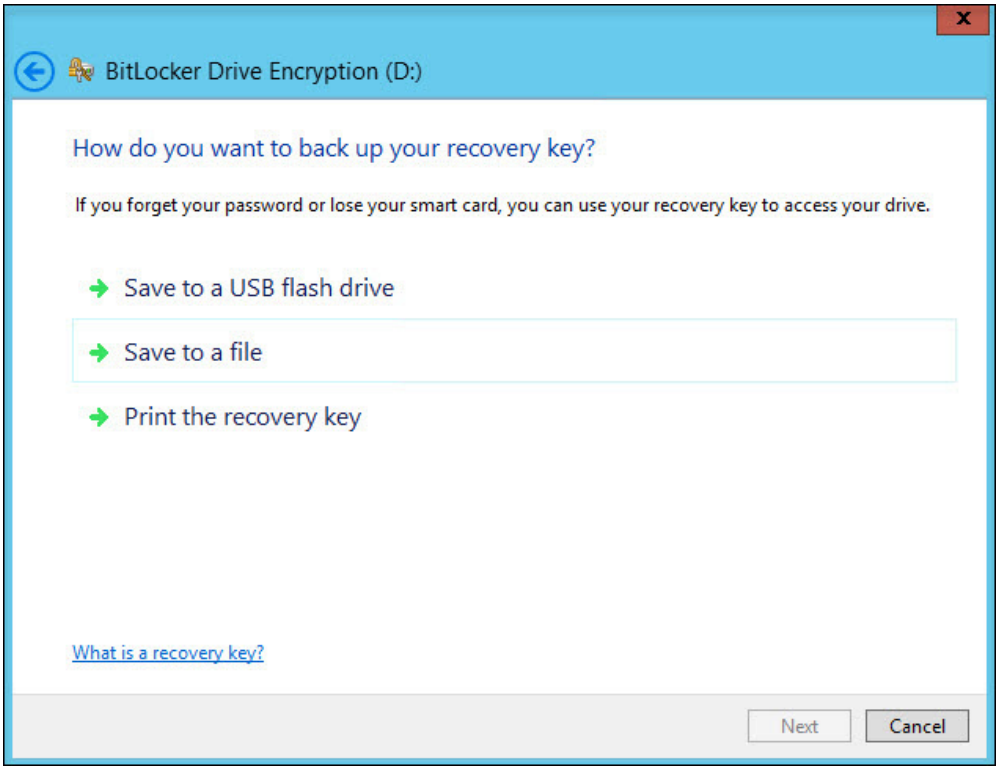
2. Как мы говорили ранее, для защиты ключа шифрования диска будем использовать токен. Важно понимать, что для использования токена или смарт-карты в BitLocker, на них должны находиться ключи RSA 2048 и сертификат.



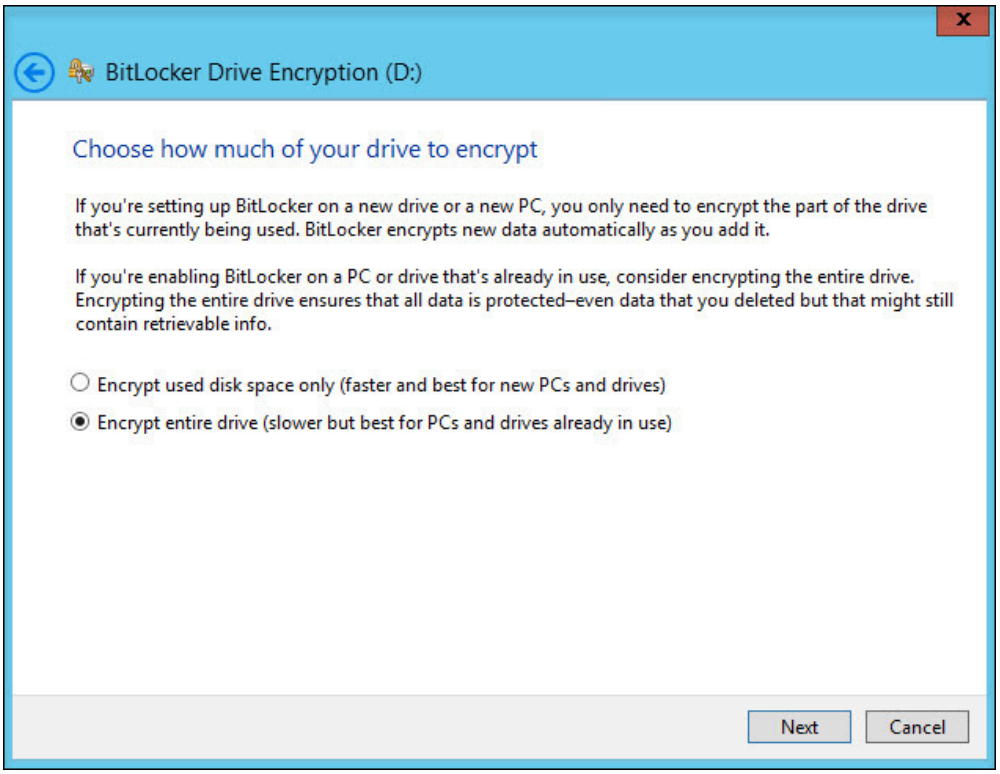
Если у вас нет домена или вы не можете изменить политику выдачи сертификатов, то можно воспользоваться запасным путем, с помощью самоподписанного сертификата, подробно про то как выписать самому себе самоподписанный сертификат описано здесь. Теперь установим соответствующий флажок.

3. На следующем шаге выберем способ сохранения ключа восстановления.





4. Далее выберем, какой режим шифрования будет использоваться, для дисков, уже содержащих какие-то ценные данные (рекомендуется выбрать второй вариант).



5. На следующем этапе запустим процесс шифрования диска. После завершения этого процесса может потребоваться перезагрузить систему. При включении шифрования иконка зашифрованного диска изменится.

4 ЗАКЛЮЧЕНИЕ

В ходе выполнения работы получили практическое освоение технологий защиты информации, научились шифровать данные на жестких дисках с помощью разных ОС.