Как мы видим, почти все отрасли подвержены утечкам информации.

Выделим основные причины утечек информации: отсутствие защиты у оператора; невнимательности самих пользователей; отсутствие чёткой нормативно-правовой базы в данной области; использование непроверенных информационных систем; утечки, связанные с поломкой или выходом из строя оборудования.

В заключение, необходимо понимать, что ответственность за защиту своих данных от утечек, несёт не только оператор, но и пользователь. Ведь именно пользователь определяет, предоставлять ли данные тому или иному оператору. Резюмируя, необходимо понимать, что утечка данных является одной из самых опасных угроз в киберпространстве. Она представляет собой действия отдельных лиц, которым удалось заполучить легитимные права доступа к информации, что привело к нарушению ее конфиденциальности. Такие действия можно разделить на две группы: преднамеренные, которые включают в себя саботаж и промышленный шпионаж, а также случайные – такие, как халатность и незнание.

***

1. Гмурман, А.И. Информационная безопасность: учебник для вузов. / А.И. Гмурман.- М.: «БИТ-М», 2014. - 387с. – ISBN 978-5-9916-6505-6

Казыханов А.А., Казыханова Д.Р., Киреева А.И.

Особенности использования современных технологий для защиты информации

*Башкирский государственный университет
(Россия, Уфа)*

doi:10.18411/lj-11-2018-148

idsp: lj-11-2018-148

Аннотация

В данной статье рассматриваются особенности использования современных технологий для деятельности по защите информации, под особенностями подразумеваются изменения, предшествующие обычным способам защиты информации без использования современных технологий

Ключевые слова: информационная безопасность, защита, информация, современные технологии

Abstract

This article discusses the features of the use of modern technologies for information protection activities, the features imply changes prior to the usual methods of protecting information without using modern technologies.

Keywords: information security, protection, information, modern technologies

Защита информации - деятельность по обеспечению основных свойств информации. В последнее время данный термин активно употребляется, причиной этому повышающийся с каждым годом интерес к области ИТ. В мире становится всё больше информации, всё большую важность информация играет для людей, именно поэтому интерес к защите информации возрастает.

С развитием технологий развиваются и способы защиты информации. Например, до повсеместной компьютеризации, много информации хранилось на бумажных источниках, и для обеспечения безопасности данной информации было необходимо только обеспечить физическую безопасность. На сегодняшний же день информация хранится в электронном виде и нуждается в большой степени защиты и по большому числу направлений защиты.

Необходимо понимать, что с информацией выполняются различные операции, соответственно, чем больше информации, тем больше с ней будет производиться операций. На рисунке, можно увидеть основные процессы, которые выполняются с информацией:

Рисунок 1. Схема - информационные процессы

С точки зрения информационной безопасности все три процесса играют огромную роль. Рассмотрим более подробно информационные процессы и влияние на них процесса защиты информации.

1. Хранение информации - данный процесс представляет собой возможность сохранить информацию и использовать её в нужное время. Так, например, любая запись на стикере - будет процессом хранения информации, также, можно отметить запись файла на флеш-накопитель или диск. Без хранения информации современный мир не сможет развиваться. С точки зрения информационной безопасности при хранении информации важно, чтобы её не изменили и не удалили. Если информация является конфиденциальной, то важно, чтобы она не стала известна третьим лицам.

2. Передача информации - эта деятельности подразумевает под собой передачу информации от одного пользователя другому или другим. Например, вышеупомянутый стикер передаётся другому человеку, и он считывает информацию с него, аналогично происходит с флеш-накопителем и диском. С точки зрения информационной безопасности, необходимо обеспечить безопасность канала передачи информации и убедиться в том, что информация передаётся именно тому пользователю, которому её хочет передать владелец.

3. Обработка информации - любые операции с информацией, которые приводят к определенным результатам важным для человека. При обработке информации для владельца информации основную роль играет результат. С точки зрения информационной безопасности в данном случае необходимо обеспечить бесперебойную обработку информации. Также, если обрабатывается информация конфиденциального характера, то необходимо обеспечить конфиденциальность информации.

В заключение отметим, основные особенности использования современных технологий для защиты информации:

- необходимость обеспечение программно-аппаратной защиты;
- защита информации становится более затратным и ёмким процессом;
- использование отдельных устройства направленных на защиту информации, например, генератор помех;
- желательность документирования процесса защиты информации;

- комплексность;
- системность.

***

1. Плотникова, Н.Г. Информатика и информационно-коммуникационные технологии (ИКТ): учебное пособие/ Н.Г. Плотникова. — М.: РИОР: ИНФРА-М, 2017. — 124 с. - ISBN 978-5-369-01308-3
2. Петраков, А.В. Основы практической защиты информации: учебное пособие/ А.В. Петраков– М.: РадиоСофт, 2015.- 504 с.- ISBN 978-5-93274-121-4

Казыханов А.А., Казыханова Д.Р., Киреева А.И.
Достоинства и недостатки при использовании USB устройства в качестве
идентификатора пользователя

*Башкирский государственный университет
(Россия, Уфа)*

doi:10.18411/lj-11-2018-149

idsp: ljjournal-11-2018-149

Аннотация

В данной статье будут рассмотрены USB идентификаторы пользователя, их назначения, достоинства и недостатки. Определить достоинства и недостатки использования USB устройств возможно на основе отзывов их использования.

Ключевые слова: информационная безопасность, USB, идентификатор, устройство

Abstract

This article will discuss the user's USB identifiers, their purpose, advantages and disadvantages. It is possible to determine the advantages and disadvantages of using USB devices based on feedback from their use.

Keywords: information security, USB, identifier, device

Защитить свои данные стремится каждый человек, именно поэтому в современном мире деятельность по защите информации занимает значимое место. Чаще всего пользователи стараются защищать свою информацию на персональном компьютере, поэтому защита информации для них сводится к защите компьютера. Деятельность по обеспечении информационной безопасности для рядового пользователя сводятся, по сути, к разграничению прав. Так пользователь создаёт две учетные записи, одну для себя и своей конфиденциальной информации, другую для гостей. Свою учетную запись пользователь защищает с помощью пароля, гостевую оставляет без защиты.

С недавнего времени, обычные пользователи помимо парольной защиты начали использовать двухфакторную аутентификацию. Это означает, что учетная запись или какие либо данные защищены двумя факторами защиты, один из них, допустим, логин-пароль, а второй код подтверждения с мобильного телефона или какой либо идентификатор предъявляемый пользователем. В роли идентификатора могут выступать различные электронные устройства, например:

- флеш-носитель;
- CD или DVD диск;
- дискета;
- Etoken;
- smart карта;
- мобильный телефон;
- умные часы;