В.В Аношкин.

V.V Anoshkin

студент 4 курса ИПИМиФ, АГПУ

(науч. рук. .Е.А. Гурова)

(науч. рук. .Е.А. Gurova)

ЗАЩИТА ИНФОРМАЦИИ В ИНТЕРНЕТЕ.

PROTECTION OF INFORMATION ON THE INTERNET.

Ключевые слова: Конфиденциальная информация, принципы защиты информации, аутентификация, целостность, секретность, административные средства защиты.

Аннотация: в этой статье автор рассказывает о методах защиты информации в интернете.

Key words: Confidential information, principles of information protection, authentication, integrity, secrecy, administrative means of protection.

Annotation: in this article, the author talks about methods of protecting information on the Internet.

В настоящее время для проведения, каких - либо операций в интернете, следует подстраховаться, обезопасить себя, соответствующим уровнем безопасности. Например: заказ товаров в интернете, использование кредитных карт при покупки товаров, закрытые информационные ресурсы, телефонные разговоры и так далее. Для этого существует конфиденциальная информация. Конфиденциальная информация, – какая - либо информация не подлежащее огласки «рассекречивания». Конфиденциальная информация проходит через определенное количество маршрутизаторов и серверов, прежде чем достигнет контрольной точки. Есть вероятность, что информацию в маршрутизаторе могут перехватить, так как сервер не контролируют, но информацию можно изменить и передать в другом виде. К большому сожалению, архитектура сети интернета желает ждать лучшего, часто информация уходит, куда не надо. Часто задается вопрос, какое выбрать необходимое оборудование и уровень защиты. Часто делают

некоторые ограничения доступу к интернету для безопасной подачи информации. На схеме 1 представлены принципы защиты информации.

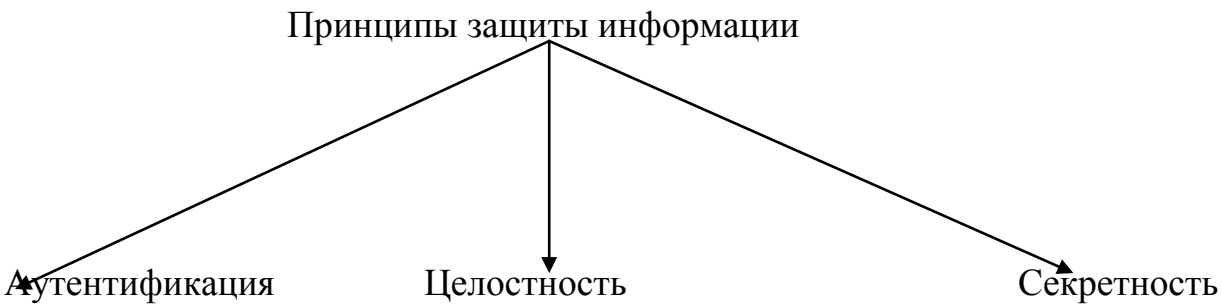

Схема 1. Принципы защиты информации

1) Аутентификация – процесс распознавания системы пользователя.
2) Целостность – сохранения данных, находящихся в исходной целостности.
3) Секретность – закрытый доступ к информации.

Утечка информации может иметь серьёзные проблемы такие как: могут отправить письмо от вашего аккаунта, электронный платеж с банковской карты и тд. Основные проблемы, которые возникают при передаче информации можно разделить на четыре группы:

1) Перехват информации – данное хранение информации нарушено.
2) Модификация информации.
3) Подмен авторство информации.
4) Перехват сообщения.

Мошенники ищут разные методы получения чужой информации, одним из распространенных методов является метод подбора. Мошенники начинают с того, что попытаются получить доступ вариантам логина, и это можно сделать путем получения почтовых аккаунтов – социальные сети, другие сайты.

Большинство почтовых сервисов и социальных сетей используют и рекомендуют двухфакторную авторизацию – сначала вводиться пароль, а следом одноразовый код. Например, такие программы: Google Authenticator или Microsoft Authenticator.

Программы Google Authenticator и Microsoft Authenticator предназначены для мобильных телефонов и требуют соединение с Интернетом.

Риски при использовании незащищенного интернета

1. Кража информации. Использования мошенниками информации в корыстных целях.
2. Подмена информации. Как и в хранилище и при передаче.
3. Программы – шпионы. Отслеживают действия на компьютере.
4. Фишинговые письма.
5. Присвоение авторства.
6. Разглашения информации.

В крупных компаниях есть специальные отделы, которые занимаются техническим обслуживанием оборудования, от внешнего проникновения.

Более мелкие компании обращаются за помощью к профессионалам или покупают лицензированный продукт. Можно выделить средства защиты:

1. Программные и технические.
2. Административные и законодательные.
3. Смешанные.

Программные средства защиты.

- Антивирусы. В задачу входит нахождения, удаления либо же изоляция программ, которые определяются, как вредоносные.
- Применения «песочниц». Это инструменты для работы с сомнительными приложениями в виртуальном пространстве.
- Брандмауэр. Программа предназначена для слежения за трафиком. В задачу входит сообщить, если на компьютер начинают поступать непонятные сигналы из непроверенных источников.

Административные средства защиты:

Рис 1. Административные средства защиты

1. Инструктаж среди сотрудников. Введения определенных правил.

2. Составления официальных договоров о неразглашении информации.

3. Создания личной системы для пользования. Каждый сотрудник имеет для программы свой логин и пароль.

4. Оптимизация набора отдела кадров. Отборка сотрудников при приеме на работу.

Часто в интернете требуется для авторизации на сервисе ввести личную почту или данные аккаунта от социальных сетей. Заведите себе дополнительный в аккаунт, который вы будете использовать для таких целей. Помните, что любая регистрация на сайтах в Интернете несет за собой СПАМ, и, если вы активный пользователь Интернета – дополнительный аккаунт – ваша защита. Внедрите такой же подход для своих сотрудников, используя метод **побуждения.**

Подведем итоги, что для защиты данных в сети интернет при помощи предлагаемых на рынке аппаратных и программных решений — можно построить эффективный и отказоустойчивый комплекс.

Но стоит помнить: все знаменитые хакеры получали доступ к данным путем работы с людьми и использования их ошибок.

Поэтому не стоит стесняться того, что на предприятии в целях безопасности до предела ограничивается свобода персонала.

Все, что может предотвратить утечки, а также разделение доступа и ответственности — способно помочь сохранить важные данные и избежать серьезных неприятностей.

Использованные источники:

1) Агальцов, В.П. Информатика для экономистов: Учебник / В.П. Агальцов, В.М. Титов. - М.: ИД ФОРУМ, НИЦ ИНФРА-М, 2016. - 448 с.

2) Балдин, К.В. Информатика и информационные системы в экономике: Учебное пособие / К.В. Балдин. - М.: НИЦ ИНФРА-М, 2016. - 218с.

3) Варфоломеева, А.О. Информационные системы предприятия: Учебное пособие / А.О. Варфоломеева, А.В. Коряковский, В.П. Романов. - М.: НИЦ ИНФРА-М, 2017. - 283 с.

4) Велихов, А. С. Основы информатики и компьютерной техники: учебное пособие / А. С. Велихов. – Москва: СОЛОН-Пресс, 2017. – 539 с.

5) Гвоздева, В. А. Информатика, автоматизированные информационные технологии и системы: учебник / В. А. Гвоздева. – Москва: Форум: Инфра-М, 2016. – 541 с.