КИБЕРБЕЗОПАСНОСТЬ В СЕТИ

CYBERSECURITY ON THE NETWORK

УДК 004

Пешева Полина Александровна, курсант Московского Университета МВД России имени В.Я. Кикотя.

Смирнов Виталий Михайлович, кандидат технических наук, старший преподаватель кафедры информатики и математики Московского университета МВД имени В. Я. Кикотя.

Pesheva P.A. pesheva368@gmail.com

Smirnov V.M. smirnov.v.m002@gmail.com

Аннотация

В современном мире кибербезопасность очень важна из-за различных угроз безопасности и кибератак. Ранее нужно было только установить антивирус на компьютер, но сегодняшние атаки являются куда более сложными и требуют специальных методов защиты. Для защиты данных множество компаний (MITRE Corporation, Symantek) разработали программное обепечение, которое защищает данные. Кибербезопаность важна, потому что она защищает не только информацию, но и всю рабочую систему от вирусной атаки.

Annotation

In the modern world, cybersecurity is very important due to various security threats and cyber attacks. Previously, it was only necessary to install antivirus on a computer, but today's attacks are much more complex and require special methods of protection. For data protection, many companies (MITRE Corporation, Symanek) have developed

software that protects data. Cybersecurity is important because it protects not only information, but also the entire working system from a viral attack.

Ключевые слова: кибербезопаность, безопасность, данные, защита, информация, сервисы, злоумышленники, сеть

Keywords: cybersecurity,security, data, protection, information, services, attackers, network

В начале развития сетей безопасность не являлась актуальной и востребованной, это было связано с тем, что в сети Интернет находился небольшой круг пользователей. На сегодняшний момент роль кибербезопасносности становится более важной в связи с тем, что компьютерные сети и Интернет захватывают все сферы жизни.

К минимальным требованиям безопасности является установка на свое рабочее место «брандмауэра», который фильтруют поступающие пакеты данных. Немаловажным является применение метода безопасного сокрытия "криптографии", для того чтобы защитить файлы, процедуры аутентификации для доступа к данным (распространенный способ — ввести код аунтентификации, биометрические проверки). Современные операционные системы снабжены алгоритмами проверки и сканирования, которые пропуская (фильтруя) различные виды информации, позволяют обеспечить основу для безопасности данных.

Кибербезопасность или как её ещё назыввают компьютерная безопасность – это совокупность практик и методов защиты от атак злоумышленников для компьютеров, мобильных устройств, электронных систем, сервисов, сетей и данных. Кибербезопасность можно встретить в разных областях и в разных направлениях, например, в бизнес-сфере, в мобильных технологиях. Также здесь можно выделить некоторые аспекты:

- Безопасная сеть – это действия по защите компьютерных сетей от различных угроз, например, от вредоносных программ.

- Безопасность приложений–это защита устройств от угроз-вирусов, которые злоумышленники могут спрятать в программах. Зараженное приложение может открыть преступнику доступ ко всем данным компьютера, которые оно должно защищать. Задолго до появления приложения в открытом доступе т.е. при создании обеспечивается его безопасность.
- Безопасность информации– это обеспечение целостности и кодификации не только во время хранения, так и при ее передаче.
- Операционная безопасность–это процесс выявления и обращение с критически важными информационными активами. К ним относятся, например, управление доступом к сети или правами определяющие хранение и передачу.
- Аварийное восстановление – это метод восстановления работоспособности инфраструктуры и доступа к ней, реагирование на действия мошенников, которое может нарушить работу систем или привести к потере данных, возникших по вине человека. Срочное пере обновление – это набор правил, которые описывают, как организация будет справляться с последствиями атаки и восстанавливать утерянные данные.
- Повышение осведомленности– это обучение пользователей сети Интернет. Данная установка сможет понизить давление самого непредсказуемого фактора в области кибербезопасности – человеческого. Ведь попасть в руки мошенника может наиболее защищенное устройство из-за нелепых ошибок. Для этого создаются специальные инструктажи для сотрудников в которых доводят важную информацию.

Какие доступные меры кибербезопасности. Чтобы сохранить свои данные и повысить безопасность самое простое что мы можем сделать-это поставить надёжные пароли и периодически их обновлять.

Мы можем использовать менеджер паролей инструмент, как LastPass, Sticky Password, чтобы отслеживать поток информации. Данные приложения помогут

нам использовать уникальные, безопасные пароли, для входа на различные сайты и вход в любые приложения. Это поможет обеспечить наиболее высокий уровень безопасности путем идентификации паролей, что усложнит попытки получения информацией. Обычно злоумышленники получают доступ к нашей сети, через старые учётные данные(записи), поэтому следует удалять неиспользуемые учётные записи. Попытайтесь удержать программное обеспечение в актуальном состоянии, тогда ваши данные всегда будут в безопасности.

На сегодняшний день из-за высокого влияния интернета на повседневную жизнь, кибербезопасность стала одной из самых востребованных потребностей в мире, ведь угрозы кибербезопасности являются серьезной проблемой общества в целом и стран мира. Не только государство, должно распространять различную информацию среди людей, но и сами граждане. Важно своевременно обновлять программы которые защищают систему(антивирус), для того чтобы наши настройки сетевой безопасности и самой системы были под защитой от вирусов.

Список использованной литературы:

1. Петренко, С. А., Ступин, Д. Д. Национальная система раннего предупреждения о компьютерном нападении: научная монография / С. А. Петренко, Д. Д. Ступин [под общей редакцией С. Ф. Боева]. – Иннополис:«Издательский Дом «Афина». – 2017. – 440 с.
2. Программа «Цифровая экономика» Российской Федерации(утверждена распоряжением Правительства РФ № 1632-р от 28.07.2017 г.)[электронный ресурс] // URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (дата обращения 15.10.2017).
3. Исследование “Экосистема Цифровой Экономики России” (2016-2017) [электронный ресурс] // URL: цифроваяэкономика.рф (дата обращения 15.10.2017).
4. Кешелава, А.В. и др. Введение в «Цифровую» экономику / А.В. Кешелава, В.Г. Буданов, В.Ю. Румянцев и др.; под общ. ред. А.В. Кешелава.– М.:

ВНИИГеосистем. - 2017. – 28 с.Петренко, С.А. и др. Цифровая экономика России и актуальность задачи импортозамещения // С.А. Петренко, К.А. Маковейчук.

References:

1. Petrenko, S. A., Stupin, D. D. National system of early warning about computer attack: a scientific monograph / S. A. Petrenko, D. D. Stupin [under the general editorship of S. F. Boev]. - Innopolis:"Publishing House "Athena". - 2017. - 440 p.
2. The program "Digital Economy" of the Russian Federation (approved by the decree of the Government of the Russian Federation No. 1632-r of 28.07.2017) [electronic resource] / / URL: http://static.government.ru/media/files/9gFM4FHj4PsB79I5v7yLVuPgu4bvR7M0.pdf (accessed 15.10.2017).
3. Research " Ecosystem of the Digital Economy of Russia "(2016-2017) [electronic resource] / / URL: digital Economy.Russian Federation (accessed 15.10.2017).
4. Keshelava, A.V. et al. Introduction to the "Digital" Economy / A.V.Keshelava, V. G. Budanov, V. Yu. Rumyantsev et al.; under the general editorship of A.V. Keshelava.-M.: VNIIGeosistem. - 2017. - 28 p.Petrenko, S. A. et al. Digital economy of Russia and the relevance of the import substitution problem / / S. A. Petrenko, K. A. Makoveychuk