Oriental Renaissance: Innovative, educational, natural and social sciences
Scientific Journal Impact Factor
Advanced Sciences Index Factor

VOLUME 2 | ISSUE 3
ISSN 2181-1784
SJIF 2022: 5.947
ASI Factor = 1.7

ИССЛЕДОВАНИЕ СЕТЕВОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

https://doi.org/10.24412/2181-1784-2022-3-1345-1353

Шораимов Хусанбой Уктамбоевич
Преподаватель кафедры «Систематическое и прикладное программирование», Ташкентский университет информационных технологий имени Мухаммеда аль-Харезми,
khusan@shoraimov.uz
Шербекова Фируза Абдурашитовна
Преподаватель Ташкентский университет информационных технологий имени Мухаммеда аль-Харезми,
fsherbekova@jmail.com
Джангазова Кумринисо Абдулвахобовна
Преподаватель Ташкентский университет информационных технологий имени Мухаммеда аль-Харезми,
qumri5544@mail.ru
Ганиходжаева Дилфуза Зиявутдиновна -
Старший преподаватель Ташкентский университет информационных технологий имени Мухаммеда аль-Харезми,
ganihodjayeva@mail.ru

АННОТАЦИЯ

Связность и открытость компьютерной сети значительно облегчают совместное использование ресурсов. Однако вместе с ростом популярности и расширением областей использования сети становятся заметными несанкционированный доступ, кража сетевых данных, хакерские атаки, вирусные атаки и ряд проблем сетевой информационной безопасности. В этом документе основное внимание уделяется необходимости законодательства, защищающего сетевую информационную безопасность, существующим правилам, а также принципам проектирования системы сетевой информационной безопасности, а также дополнительно исследуются меры предосторожности в отношении сетевой информационной безопасности.

Ключевые слова: *сетевая информационная безопасность, законодательство, принципы проектирования превентивные меры.*

ABSTRACT

The connectivity and openness of a computer network greatly facilitates the sharing of resources. However, along with the growing popularity and expansion of the areas of use of the network, unauthorized access, theft of network data, hacker attacks, virus attacks and a number of network information security problems are becoming noticeable. This paper focuses on the need for legislation to protect network information security, existing regulations, and network information security system design principles, and further explores network information security precautions.

Keywords: *network information security, legislation, design principles, preventive measures.*

ВВЕДЕНИЕ

Быстрое развитие и широкое использование Интернета привели людей в совершенно новый информационный век. Интернет, который сильно повлиял и изменил образ жизни людей, проникает в политику, экономику и все общество. От правительства, предприятий до любого человека зависимость от киберпространства становится все более и более естественной. Нормальная работа интернета является залогом общественного порядка, и, как следствие, безопасность информации в Интернете становится очень важным вопросом. Тем более, что в «призме» Откровения все правительства считают сетевую информационную безопасность главным приоритетом.

В июне 2013 года Washington Post и Guardian раскрыли некоторую конфиденциальную информацию о проекте агентства национальной безопасности. Проект под кодовым названием «PRISM» был опубликован подрядчиком АНБ Эдвардом Сноуденом, который охарактеризовал масштабы массового сбора данных как «опасную» и «преступную» деятельность. На этом основании тайное поведение правительства США, использующего большие многонациональные сетевые группы для наблюдения за частной сетевой информацией людей, было разоблачено и представлено общественности. Разоблачение проекта "PRISM" встревожило правительства всего мира, и это заставило их серьезно отнестись к сетевой информационной безопасности.

ОБСУЖДЕНИЕ И РЕЗУЛЬТАТЫ

Сетевая информационная безопасность - это всеобъемлющая дисциплина, связанная с информатикой, сетевыми технологиями, коммуникационными технологиями, технологиями информационной безопасности, технологиями

паролей, прикладной математикой, информатикой и другими междисциплинарными дисциплинами. Его целью является защита данных компьютерного оборудования, программного обеспечения и системы от изменения, раскрытия, уничтожения, а также поддержание нормальной работы сетевой системы.

Необходимость законодательства для защиты сетевой информационной безопасности и существующие законы и правила

А. *Необходимость законодательства для защиты сетевой информационной безопасности*

В современном мире сетевой информации время от времени происходит ряд событий, связанных с сетевой информационной безопасностью, таких как несанкционированный доступ, нарушение целостности данных, глушение работы системы, передача вируса по сети, прослушивание линий, незаконное раскрытие и использование личной информации, а также онлайн-мошенничество. . Следующие аспекты, от коммерческой тайны и управления до личной жизни и собственности, а также национальной безопасности и развития, находятся под серьезной угрозой. Законодательство для защиты безопасности сетевой информации является обязательным.

Каждый несет ответственность за обеспечение безопасности сетевой информации, и действия должны основываться на законе и мерах безопасности. Каждый имеет право пользоваться Интернетом и в то же время должен нести соответствующие обязанности. В сетевом мире люди также должны придерживаться морали и справедливости, не должны нарушать другие права и интересы или нарушать работу сети просто в корыстных целях. Сетевое законодательство и гражданские права тесно связаны между собой. С большой уместностью это способствует очищению сетевой среды для положительной роли сети. При осуществлении радикального решения сетевых проблем должна быть создана общая система механизма защиты информации.

В целом нынешние правовые нормы, связанные с защитой сетевой информации, относительно слабы и отстают, значительно отстают от требований развития информатизации нашей страны и обеспечения законных прав и интересов граждан в сетевой деятельности. Его следует дополнительно улучшить.

Принцип построения сетевой системы защиты информации

В соответствии с национальными общими правилами безопасности построение сетевой системы информационной безопасности должно следовать следующим принципам.

A. Принцип честности

Прежде всего, проектирование системы информационной безопасности компьютерной сети следует начинать со всей перспективы. Он должен следовать принципу общей безопасности, всесторонне рассматривая каждый объект и каждое звено, которое охватывает безопасность информационной сети, избегая возникновения дефектов и слабых звеньев, создавая совершенную систему сетевой безопасности. В частности, следует внимательно рассмотреть следующие аспекты: правовая политика, система управления (рабочий процесс, обучение персонала, техническое обслуживание и т. д.), технические меры защиты (технология распознавания, контроль доступа, шифрование, защита от вирусов и т. д.). Система защиты информации сети должна включать в себя механизм защиты безопасности, механизм мониторинга безопасности и механизм восстановления безопасности.

B. Принцип последовательности и стандартизации

Принцип непротиворечивости в основном относится к непротиворечивости системы сетевой информационной безопасности требованиям сетевой безопасности. Дизайн системы безопасности, сетевая аутентификация и работа должны быть оснащены стандартизированными мерами безопасности.

C. Принцип периодичности

В связи с изменением времени, среды и средств сетевых атак система защиты сетевой информации не могла стоять на месте, приобретая периодические характеристики. Соответствующая базовая система безопасности должна основываться на изменяющейся ситуации в сети, а дополнительные защитные меры должны быть усилены при обновлении изменений.

D. Принцип практичности

Практичность или работоспособность следует учитывать при разработке системы защиты сетевой информации. Требование к уровню компьютерных знаний пользователя может быть не слишком высоким. Вычурный дизайн не будет выгодно популяризировать и применять.

E. Принцип иерархии

Чтобы удовлетворить фактические потребности для различных уровней сети, безопасность системы сетевой информационной безопасности должна быть выровнена в соответствии с различными объектами, такими как классификация разрешений на операции пользователей (индивидуальные и групповые), классификация архитектуры реализации системы (прикладной уровень, сетевой уровень). , канальный уровень и др.), классификация конфиденциальности информации (совершенно секретно, конфиденциально, секретно).

F. Принцип многократной защиты

Система сетевой информационной безопасности должна устанавливать множественную защиту , чтобы играть защитную роль при возникновении нарушений сетевой информационной безопасности и, в конечном итоге, предотвращать ее нарушение. Когда значительная защитная мера не работает, можно инициировать другой уровень, чтобы избежать или минимизировать потери.

Меры предосторожности в отношении сетевой информационной безопасности

Меры предосторожности в отношении сетевой информационной безопасности касаются технологий, персонала и руководства. Далее основное внимание уделяется техническим аспектам превентивных мер.

A. Технология брандмауэра

Технология брандмауэра относится к изоляции между локальной сетью и системой защиты внешней сети. Он устанавливает шлюз безопасности между Интернетом и Интранетом, чтобы блокировать вторжение из внешней сети. Это контроль порога связи с обеих сторон.

Брандмауэр — очень эффективная модель сетевой безопасности в Интернете, с помощью которой можно изолировать зону риска и зону безопасности от соединения. Только безопасная и проверенная информация может быть доступна. Технология брандмауэра обычно основана на технологии фильтрации пакетов, а стандарт фильтрации пакетов формулируется на основе политики безопасности. В настоящее время основной брандмауэр включает в себя брандмауэр с фильтром пакетов, прокси-брандмауэр и комплексный брандмауэр. Полный комплект системы брандмауэра состоит из защиты маршрутизатора и прокси-сервера. Брандмауэр с фильтром пакетов относится к фильтру пакетов или фильтру пакетов с группировкой данных. Принцип и технологию фильтрации пакетов можно рассматривать как основу различных

сетевых брандмауэров. Прокси-брандмауэр — это изолированная точка интрасети и экстрасети, играющая роль мониторинга и изоляции от коммуникационного потока прикладного уровня. Комплексный межсетевой экран используется совместно с фильтрацией пакетов и прокси-сервисом.

Роль раннего брандмауэра заключается в защите хоста и усилении контроля доступа. Тем не менее, текущий брандмауэр разработан с функциями шифрования, дешифрования, сжатия, распаковки и других. Это повысило безопасность сетевой информации.

B. Технология обнаружения вторжений

В отношении сетевых вторжений технология обнаружения вторжений имеет важное значение. Брандмауэр просто пытается противостоять захватчикам. Трудно найти попытки вторжения и успешное вторжение, но технология обнаружения вторжений эффективно восполняет пробелы. Технология обнаружения сетевых вторжений может обнаруживать вторжение и попытку вторжения, своевременно предупреждая пользователей для предотвращения вторжения. Тип системы обнаружения вторжений можно разделить на хост-систему обнаружения вторжений, сетевую систему обнаружения вторжений и распределенную систему обнаружения вторжений в зависимости от источника.

C. Технология шифрования данных

Используя цифровой метод для реорганизации данных, технология шифрования данных делает невозможным восстановление исходной информации другими лицами, кроме законных посетителей. Применение технологии шифрования данных является ядром сетевой информационной безопасности, а парольные средства обеспечивают надежную гарантию. Цифровая подпись и аутентификация на основе пароля являются одними из основных методов обеспечения целостности информации. Появление технологии шифрования гарантирует глобальную электронную коммерцию, что делает возможным создание электронной торговой системы на базе Интернета.

D. Управление доступом в сеть

Контроль доступа к сети является одной из основных стратегий сетевой безопасности и защиты, включая различные методы контроля, такие как доступ к сети, разрешения, каталог и свойства. Одним из средств управления допуском в Сеть является аутентификация личности. Это один из видов проверки согласованности, в основном включающий основу аутентификации, систему аутентификации и требования безопасности. Вход в сеть — это первый этап

контроля доступа к сети, обычно посредством проверки учетной записи пользователя и пароля для контроля несанкционированного доступа. Учетные записи пользователей и пароли должны быть строго регламентированы, например: пароль и номер учетной записи должны быть достаточно длинными; цифры и буквы (с учетом регистра) или символы должны быть смешаны; избегайте использования общего цифрового пароля в качестве номера дня рождения или идентификационного номера; Пароль должен быть максимально сложным и регулярно обновляться, чтобы предотвратить его кражу. В настоящее время широко используемая технология идентификации в основном основана на системе аутентификации, авторизации и управления (AAA) RADIUS. Второй метод управления доступом в сеть — это контроль доступа. Он управляет субъектом какого-либо объекта с помощью силы. Контроль доступа включает тип идентификации данных, контроль доступа, контроль типа, ограничения персонала и анализ рисков. Технология контроля доступа и аутентификации обычно используется вместе, предоставляя разные полномочия для разных идентификаторов пользователей для достижения разных уровней безопасности управления классификацией информации.

E. Виртуальная частная сеть (VPN)

Функции виртуальной частной сети: создание выделенной сети в общедоступной сети; осуществлять зашифрованную связь. Он широко используется в корпоративной сети. Функции VPN-шлюза основаны на шифровании пакетов и преобразовании целевого адреса для осуществления удаленного доступа. VPN имеет множество классификаций, в основном классифицируемых в соответствии с соглашением, и может быть реализован через сервер, оборудование, программное обеспечение и так далее. VPN устанавливает специальное логическое соединение через общедоступную сеть, позволяя пользователям получать доступ во внутреннюю сеть из разных мест с теми же ресурсами, что и при локальном доступе, не беспокоясь о проблеме утечки.

F. Резервное копирование и восстановление базы данных

Информационная безопасность сети требует тщательной подготовки. Чтобы профилактика была на первом месте, пользователи должны выработать привычку создавать резервные копии важных данных в любое время и обращать внимание на то, чтобы система работала все время. Резервное копирование и восстановление базы данных — важная операция администратора базы данных для обеспечения безопасности и целостности

данных. Резервное копирование — это эффективный способ восстановления базы данных, но восстановление — это восстановление исходных данных после аварии с использованием резервной копии.

Помимо мер технической защиты очень важна профилактика со стороны персонала и руководства. Персонал должен быть обучен безопасности сетевой информации, чтобы предотвращать компьютерные преступления и повышать осведомленность о предотвращении. На уровне управления необходимо установить полную систему управления сетевой информационной безопасностью. Компьютерные комнаты, файлы, контроль, эксплуатация и техническое обслуживание должны быть строго разделены для организации труда.

ЗАКЛЮЧЕНИЕ

Сетевая информационная безопасность представляет собой сложную системную инженерию, включающую в себя законодательную защиту, персонал, технологии, оборудование, управление и другие аспекты факторов. Система защиты информации в сети должна быть настроена как единое целое. Сетевая информационная безопасность представляет собой комбинацию технологии брандмауэра, шифрования данных и контроля доступа, чтобы сформировать полный набор скоординированной системы защиты сетевой безопасности. Помимо технологий, нам необходимо усилить управление, усовершенствовать законодательство по сетевой информационной безопасности, повысить интенсивность правоприменения и сформулировать соответствующие стандарты безопасности. Благодаря вышеуказанным мерам сеть может лучше служить человеческому обществу.

REFERENCES

1. Daoyuan. Hu, Network Technology Tutorial. Beijing: Tsinghua University Press,2015.
2. Shibin. Zhang,Network Security Technology. Beijing: Tsinghua University Press,2015.
3. Tianjie. Cao, Computer System Security. Beijing:Higher Education Press, 2013.
4. Maozhi. Xu, Introduction to Information Security. Beijing:Posts and Telecom Press,2017.
5. V. Vargas, A. Syed, A. Mohammad, and M. N. Halgamuge, "Pentaho and Jaspersoft: A Comparative Study of Business Intelligence Open Source Tools

Processing Big Data to Evaluate Performances", Int. Journal of Advanced Computer Science and Applications (IJACSA), vol 7, no 10, pp. 20-29, November 2016.
6. N. Nissim, R. Moskovitch, L. Rokach and Y. Elovici, “Detecting unknown computer worm activity via support vector machines and active learning”, Pattern Analysis and Applications, vol 15, no. 4, pp. 459-475, 2017.
7. P. Szor, “The art of computer virus research and defense”, Pearson Education, 2017.
8. A. Aziz, U.S. Patent No. 8, Washington, DC: U.S. Patent and Trademark Office, pp. 516,593, 2013.
9. M. E. Newman, S. Forrest, J. Balthrop, “Email networks and the spread of computer viruses”, Physical Review E, vol. 66, no. 3, 2012.
10. F. Cohen, “Computer viruses: theory and experiments”, Computers & security, vol. 6, no. 1, pp. 22-35. 2017.