УДК 004 **DOI: 10.34670/AR.2023.86.75.035**

Стратегии информационной безопасности и защиты компьютерных сетей: экономические аспекты

Чажаева Майнат Маусуровна

Кандидат экономических наук,
доцент кафедры государственного и муниципального управления,
Чеченский государственный университет им. А.А. Кадырова,
364093, Российская Федерация, Грозный, ул. Асланбека Шерипова, 32;
e-mail: mchajaev@mail.ru

Халиева Хава Сеитхамзатовна

Старший преподаватель,
Грозненский государственный нефтяной технический университет,
364024, Российская Федерация, Грозный, пр. Исаева, 100;
e-mail: Hava_ggni@mail.ru

Магомадова Зарина Саидбековна

Старший преподаватель кафедры «Прикладная информатика»,
Чеченский государственный педагогический университет,
364051, Российская Федерация, Грозный, пр. Исаева, 62;
e-mail: Mrs-70@mail.ru

Аннотация

Компьютерные технологии широко применяются в окружающей среде, способствуя развитию и изменениям в различных отраслях. В то же время технология также развивается и модернизируется. В эпоху Интернета на сетевых объектах собирается большой объем информации, при этом необходимо обеспечить безопасную работу оборудования, что имеет большое значение для безопасности общедоступных данных и информации. На этом этапе предприятия ускоряют строительство и развитие информационных сетей. Многие предприятия хранят данные в сетевых объектах, тем самым повышая эффективность офиса и качество работы предприятий. На фоне новой эпохи в данной статье сначала анализируется уровень сетевой безопасности и оценка рисков компьютеров, рассматриваются конкретных проблемы безопасности компьютерных сетей в новую эпоху, а также предлагаются конкретные планы защиты компьютерной сети. С появлением сетевой информатизации и эпохи больших данных надежность и безопасность компьютерных информационных технологий постепенно стали в центре внимания. На этом фоне протоколы сетевой безопасности начали постепенно применяться к технологиям компьютерной связи, и были замечены хорошие результаты. Однако в реальном процессе подачи заявки были обнаружены определенные недостатки, что требует от соответствующего технического персонала постоянно учиться на основе

опыта и извлеченных уроков, стремиться к совершенствованию и улучшению текущих протоколов сетевой безопасности, обеспечивать коммуникационную безопасность компьютерных сетей и способствовать развитию экономики.

Для цитирования в научных исследованиях

Чажаева М.М., Халиева Х.С., Магомадова З.С. Стратегии информационной безопасности и защиты компьютерных сетей: экономические аспекты // Экономика: вчера, сегодня, завтра. 2023. Том 13. № 9А. С. 581-589. DOI: 10.34670/AR.2023.86.75.035

Ключевые слова

Компьютерная сеть, технология безопасности, шифрование, информационные технологии, протоколы сетевой безопасности.

Введение

В эпоху информационных сетей компании ускоряют применение информационных сетей для повышения своей производительности и конкурентоспособности на рынке. В виртуальной сетевой среде вопросы информационной безопасности данных занимают очень важное место, в то же время они расширяются с увеличением масштабов Интернета и угрожают информационной безопасности предприятий и частных лиц. Анализ показывает, что среда сетевых приложений очень сложна.

Основная часть

В настоящее время заметны проблемы сетевой информационной безопасности, такие как инструменты взлома, распространение троянских коней и т.д. Под влиянием многих угроз безопасность и непрерывность сетевой передачи не могут быть нарушены. Использование уязвимостей системы для удаленного управления пользовательскими устройствами, а также кражи и повреждения пользовательской информации, очевидно, приведет к тому, что компании понесут большие потери, если это строго конфиденциальная информация [Таненбаум, 2012].

С быстрым развитием модели электронной коммерции корпоративные онлайн-офисы стали тенденцией, и в это время проблемы безопасности корпоративных сетевых приложений стали более заметными. При применении компьютерных сетевых систем мы сталкиваемся со многими рисками. Существование угроз безопасности является основной причиной проблем безопасности.

Согласно анализу, риски безопасности сетевых систем включают, в частности, бэкдоры, вирусы, системы и т.д. Другими словами, безопасность компьютерных сетевых систем в конечном итоге должна определяться конкретной средой, обеспечиваемой операционной системой и аппаратными устройствами. Осведомленность пользователей об информационной безопасности относительно слаба, они не уделяют достаточного внимания сетевой информационной безопасности, а меры управления отсутствуют, что приводит к сбоям в безопасности.

Пользовательские риски в основном отражаются в учетных записях пользователей, ролях и разрешениях на операции, предоставленных конкретным объектам компьютерной сети. Например, формы доступа и этапы хранения. В сегодняшних широко используемых

операционных системах и компьютерных сетевых системах особенно важные функции безопасности не предусмотрены, а большинство связанных компьютерных сетевых систем недостаточно развиты [Грибунин, Чудовский, 2009].

После проведения многоаспектного анализа текущих рисков сетевой безопасности можно проанализировать текущие технические меры сетевой безопасности, такие как технология сетевой безопасности, технология управления хранилищем, технология резервного копирования и восстановления, а также создание механизма безопасного аудита. Конкретный анализ заключается в следующем:

Идентификация пользователя основана на авторизации в компьютерной сети. Законными пользователями являются только авторизованные пользователи, прошедшие проверку личности в компьютерной сети. Существует множество технологий авторизации в компьютерных сетях, таких как системное чтение и запись, технологии запроса и изменения информации и т. д.

Технология контроля доступа существует для лучшей защиты данных сетевой системы. Когда пользователь входит в систему, он или она может получить доступ к данным данных только с соответствующими разрешениями. Система будет контролировать контент, к которому пользователь получает доступ, на основе настроек [Кравец, Кукарцев, Сенашов, 2012]. Его основная технология в основном опирается на систему безопасности компьютерной сети, и это наиболее эффективный метод безопасности. Посетители могут использовать выполнение соответствующих программ для контроля доступа, тем самым гарантируя, что риски безопасности находятся в пределах разумного уровня [Сергеев, 2016]. Пользователи доступа, если они авторизованы на данный момент, могут выполнять ряд операций с данными в сетевой системе.

Что касается обычных пользователей, то их доступ в настоящее время ограничен, и они не могут совершать операции по контролю данных по своему желанию. Этот функциональный модуль использует авторизацию соответствующих пользователей, так что каждый модуль соответствует соответствующему пользователю. Существуют различия в разрешениях каждого пользователя. Как правило, пользователи могут только запрашивать и обновлять. Не все функции могут быть использованы, и функциональный модуль имя, имя пользователя и разрешения тоже. Код можно сохранить в той же компьютерной сети.

Основные проблемы, существующие в сфере информационной безопасности компьютерных сетей:

1. Уровень защищенности компьютерных сетей низкий.

В списке приоритетов находятся некоторые процедуры кибербезопасности, которые абсолютно необходимы. Компьютерные сети должны иметь высокую доступность, чтобы обеспечить бесперебойную разработку приложений [Оливейн, 2004]. В массовой базе данных будет храниться личная информация, которую можно будет обрабатывать в соответствии с реальными потребностями. Однако при низкоуровневых мерах защиты хакеры могут легко проникнуть в базу данных, и для решения проблемы необходимо усилить защиту структурированных данных.

В настоящее время общей проблемой является то, что у общественности недостаточно понимания информации, которую необходимо защищать, и ее классификации, что приводит к некоторым потерям данных. Видно, что в современных сетевых приложениях уровень защиты сетевой безопасности относительно низок, что обеспечивает благоприятные условия для формирования проблем сетевой информационной безопасности.

2. Имеются лазейки в надзоре за компьютерными сетями.

В настоящее время при разработке сетевых приложений существует множество серьезных проблем с надзором за сетевой безопасностью. Согласно анализу, это связано с тем, что общественность менее чувствительна к цифровой информации. В настоящее время, сталкиваясь с этими случаями информационной безопасности, невозможно определить, существует ли конфиденциальная информация. Будучи измененной или утерянной, это, очевидно, лазейка в регулировании.

Под влиянием регуляторных проблем было скопировано много конфиденциальных данных и информации, но в то время невозможно было судить о сетевой безопасности. В сети при тестировании новых обновлений кодовой системы будет напрямую копироваться большой объем данных, собранных исходной системой. Однако содержимое сетевой системы трудно судить и анализировать во время обновлений системы, исправлений и т.д., и невозможно сделать точные суждения об истинном назначении данных. Поэтому необходимо углубить понимание эксплуатационной безопасности для лучшей защиты безопасности данных.

В реальных операциях некоторые преступники используют уязвимости сетевой системы для проведения целенаправленных атак и обработки, тем самым успешно вторгаясь в систему, похищая и уничтожая информацию в сетевой системе, а также нанося разную степень ущерба учетным записям пользователей [Кукарцев, Шеенок, 2013]. Видно, что в нынешнем сетевом надзоре есть лазейки, и эти лазейки дают преступникам возможность воспользоваться и способствовать формированию проблем сетевой информационной безопасности.

3. Неоднозначные права доступа к компьютерным сетям.

В настоящее время настройка разрешений на доступ к сети в основном предназначена для сетевых приложений учреждений. Для построения сетевых систем муниципальных управлений, департаментов и т.д., поскольку ресурсы относительно достаточны во всех аспектах, они постепенно развиваются и созревают в рамках эффективного сотрудничества.

Однако в некоторых низовых учреждениях из-за таких факторов, как недостаток специалистов, низовые учреждения в основном приобретают сетевое системное оборудование и системы непосредственно у малых предприятий на рынке. Сотрудники этих малых предприятий обладают определенными навыками. Однако их профессионализм недостаточен, и они относительно мало знают конфиденциальную информацию, поэтому построенная ими сетевая система имеет проблемы с безопасностью.

При этом в сетевой системе, построенной на низовом уровне, большинство пользователей могут напрямую войти в систему, используя простые пароли, что вызывает проблемы с безопасностью сетевой информации, при этом отсутствует доступ к ключевой информации в системе. Разрешения: все пользователи могут запрашивать любую информацию в системе, что обнажает проблему неоднозначных прав доступа к сетевой системе [Тынченко, Сахалтуева, Платонова, 2016].

4. Система управления информационной безопасностью компьютерной сети несовершенна.

Для эффективной работы сетевой информационной системы, созданной организацией, необходимо построить полную системную безопасность. Это также верно для управления сетевой информационной безопасностью. На ранних этапах развития сети предприятия могут построить систему, отвечающую их собственным потребностям, способствовать эффективному соединению внутренних задач и поддерживать безопасную работу сети [Максимов, 2003].

Однако среда времени претерпевает быстрое развитие и изменение. Широкомасштабное применение сети привело к огромным изменениям в развитии и работе предприятий. Если предприятия не идут в ногу со временем и не укрепляют сети системы управления

информационной безопасностью, в это время в сети будет легко выйти из строя, системное приложение понесет большие потери и даже приведет к краху предприятия. Почему это происходит? Это было в основном вызвано несовершенством системы управления сетевой информационной безопасностью предприятия. Подробный анализ выглядит следующим образом:

Во-первых, в новую эпоху сетевых коммуникаций традиционная модель доставки больше не может идти в ногу со временем. Руководство некоторых компаний закрывает глаза на бурное развитие компьютерных технологий, полагает, что успеха можно достичь за счет максимизации технологии, пренебрегает анализом проблем на основе реальных условий, что приводит к ошибкам в принятии решений. Так обстоит дело и с Kodak: даже несмотря на бурное развитие цифровых фотоаппаратов, она все еще цепляется за пленочные фотоаппараты, в конечном итоге упав из некогда знаменитого гиганта в бесконечную пропасть [Кулягин и др., 2015].

Во-вторых, существуют недостатки в менеджерах по безопасности компьютерных сетей на техническом уровне. В настоящее время компании всегда просят старых сотрудников руководить новыми сотрудниками. Это имеет определенные преимущества с точки зрения понимания рабочей среды компании, но есть и хорошие, и плохие аспекты. Недостаток заключается в том, что старые сотрудники, как правило, старше и не могут понимать новейшие компьютерные теории и технологии в режиме реального времени. Они по-прежнему используют свою собственную логику.

В-третьих, конкурентные отношения между компаниями. В условиях постоянного расширения компьютерной сферы большинство компаний открыли свои собственные сетевые каналы не только для того, чтобы соответствовать тенденциям времени и ускорить собственное развитие, но и в надежде получить большую выгоду. Конкуренция среди компаний в компьютерной сфере становится все более жесткой. Некоторые компании слишком осторожны, в результате чего они мало общаются с другими компаниями или даже закрываются, чтобы достичь цели защиты своих важных ресурсов данных, но они также игнорируют анализ общей ситуации на рынке и теряют инновации, тем самым заставляя себя медленно отставать и в конечном итоге претерпевать неудачу из-за непонимания рынка, неспособности уловить соответствующие рыночные тенденции и отсутствия исследований новых технологий.

5. Система внутреннего контроля и управления информационной безопасностью компьютерных сетей несовершенна.

Во время разработки системы инженеры часто оставляют некоторые лазейки в системе, чтобы облегчить последующие обновления и улучшения системы. Помимо этих уязвимостей, несовершенные системы внутреннего контроля сетевой информационной безопасности также подвергают данные угрозам безопасности.

Меры по защите информационной безопасности компьютерных сетей:

1. Создать систему защиты безопасности компьютерной сети.

На этом этапе система защиты базы данных обычно имеет три аспекта: обнаружение уязвимостей, классификация данных и авторизация защиты. Ниже приведен их более подробный анализ:

1. Обнаружение уязвимостей.

На основе анализа с точки зрения DLP (предотвращения потери данных) установлено, что данные очень важны. В основном для определения этого файла, а также пользователя и владельца файла. Для защиты файлов лучшей стратегией является сканирование серверов и сетевых устройств. С помощью сканирования мы можем определить процесс производства,

способы хранения, доступа, изменения, передачи и т.д., а затем выполнить действия по обнаружению и идентификации для анализа статических и динамических данных.

2. Градуированные данные.

Использовать некоторые стратегии для поиска, классификации и организации статических данных в сетевых системах. Расширенное программное обеспечение для обнаружения сети может собирать информацию о всей сети, находить компьютерные сети, соответствующие условиям. При регулярном сканировании сетевых систем, если законы и правила часто нарушаются, выдается предупреждение и требуются исправления. Индекс данных и схема ранжирования обеспечивают людям большое удобство в понимании и использовании данных, а также могут получать информацию о местоположении. Кроме того, данные сети общественной безопасности в настоящее время будут шифроваться и регулярно создаваться резервные копии.

3. Разрешение на защиту.

Нам также необходимо понимать динамические данные, проходящие через сеть, что также является важной частью эффективного исследования данных. Технология захвата работает путем сбора и записи сетевого трафика в течение длительного периода времени. Они анализируют типы данных для выявления стандартных и частных данных, а затем разрабатывают эффективные политики для предотвращения и контроля потока данных за пределами сети. Если мы хотим защититься от инсайдеров, вы должны зашифровать свои данные. Если устройство потеряно или украдено, нам также необходимо предотвратить несанкционированный доступ других лиц.

2. Улучшить технологию многорежимного шифрования компьютерной сети.

Для компьютерной сети или самих данных лучшей стратегией защиты является шифрование. Благодаря специальной технологии шифрования, когда данные просачиваются под воздействием различных факторов, защита шифрования по-прежнему может играть определенную защитную роль, так что реальная информация о данных не будет легко раскрыта.

С быстрым развитием информационных технологий меры безопасности и защиты также меняются и развиваются с высокой скоростью. В условиях быстрых изменений сетевой среды технология многорежимного шифрования является лучшим методом. При использовании этой технологии используются симметричные и асимметричные алгоритмы, позволяющие улучшить качество шифрования и сделать шифровальную защиту очень гибкой [Гольдштейн, 2005]. При использовании этой технологии можно свободно выбирать режим шифрования. Следовательно, соответствующую технологию шифрования необходимо выбирать с учетом соответствующих потребностей окружающей среды. Чтобы удовлетворить потребности в шифровании нескольких типов данных, эта технология устраняет ограничения защиты формата и значительно повышает общий уровень защиты шифрования.

3. План предотвращения безопасности корпоративной сети

Для приложений сетевых систем очевидно, что чем больше сервисов, тем больше проблем с безопасностью. Отключив те конфигурации и меры защиты, которые не включены в политику сетевой безопасности, тем самым предоставляя пользователям минимальные права использования, это может значительно снизить риски безопасности системы и уменьшить угрозы безопасности сетевой системы. В сетевой среде, если не настроена конкретная политика управления безопасностью, чтобы снизить риск вторжения, сетевые менеджеры обычно прерывают обмен информацией и данными с неизвестными сетями, тем самым предотвращая риски, которые могут возникнуть в процессе передачи.

Заключение

Подводя итог, с появлением сетевой информатизации и эпохи больших данных надежность и безопасность компьютерных информационных технологий постепенно стали в центре внимания. На этом фоне протоколы сетевой безопасности начали постепенно применяться к технологиям компьютерной связи, и были замечены хорошие результаты. Однако в реальном процессе подачи заявки были обнаружены определенные недостатки, что требует от соответствующего технического персонала постоянно учиться на основе опыта и извлеченных уроков, стремиться к совершенствованию и улучшению текущих протоколов сетевой безопасности, обеспечивать коммуникационную безопасность компьютерных сетей и способствовать развитию экономики.

Библиография

1. Гольдштейн Ф.Б., Гольдштейн Б.С. Технология и протоколы MPLS. СПб.: БХВ-Петербург, 2005. 304 с.
2. Грибунин В.Г., Чудовский В.В. Комплексная система информационной безопасности на предприятии. М.: Академия, 2009. 416 с.
3. Кравец А.А., Кукарцев В.В., Сенашов С.И. Организация информационной системы сбора данных по медицинской помощи на территории края // Актуальные проблемы авиации и космонавтики. 2012. № 8. С. 396-397.
4. Кукарцев В.В., Шеенок Д.А. Оптимизация программной архитектуры логистических информационных систем // Логистические системы в глобальной экономике. 2013. № 3. С. 138-145.
5. Кулягин В.А. и др. Концептуальная модель многоэтапной комплексной оценки надежности автоматизированных систем управления предприятиями // Фундаментальные исследования. 2015. № 7-2. С. 323-327.
6. *Максимов* В. Межсетевые экраны. *Способы организации защиты* // Компьютерпресс. *2003. № 3. С. 68*.
7. Олвейн В. Структура и реализация современной технологии MPLS. М.: Вильямс, 2004. 480 с.
8. Сергеев А.Н. Основы локальных вычислительных сетей. СПб.: Лань, 2016. 184 с.
9. Таненбаум Э. Компьютерные сети. СПб.: Питер, 2012. 960 с.
10. Тынченко В.С., Сахалтуева Ю.С., Платонова О.В. Применение OLAP-технологий в управлении предприятием // Экономика и социум. 2016. № 12-3. С. 86-88.

Information security and computer network protection strategies: economics aspects

Mainat M. Chazhaeva

PhD in Economics,
Associate Professor of the Department of State and Municipal Administration,
Chechen State University,
364049, 32, Sheripova str., Grozny, Russian Federation;
e-mail: mchajaev@mail.ru

Khava S. Khalieva

Senior Lecturer,
Grozny State Oil Technical University,
364024, 100, Isaeva ave., Grozny, Russian Federation;
e-mail: Hava_ggni@mail.ru

Zarina S. Magomadova

Senior Lecturer of the Department of Applied Informatics,
Chechen State Pedagogical University,
364068, 62, Isaeva ave., Grozny, Russian Federation;
e-mail: Mrs-70@mail.ru

Abstract

Computer technologies are widely used in the environment, contributing to the development and changes in various industries. At the same time, the technology is also being developed and modernized. In the era of the Internet, a large amount of information is collected at network facilities, while it is necessary to ensure the safe operation of equipment, which is of great importance for the security of publicly available data and information. At this stage, enterprises accelerate the construction and development of information networks. Many enterprises store data in network objects, thereby increasing the efficiency of the office and the quality of work of enterprises. Against the background of the new era, this article first analyzes the level of network security and risk assessment of computers, discusses specific problems of computer network security in the new era, and also offers specific plans for protecting a computer network. With the advent of network information technology and the era of big data, the reliability and security of computer information technology has gradually become the focus of attention. Against this backdrop, network security protocols have gradually begun to be applied to computer communication technologies and good results have been observed. However, certain shortcomings have been found in the actual application process, which requires relevant technical personnel to continuously learn from experience and lessons learned, strive to improve and improve current network security protocols, ensure the communication security of computer networks, and promote economic development.

For citation

Chazhaeva M.M., Khalieva Kh.S., Magomadova Z.S. (2023) Strategii informatsionnoi bezopasnosti i zashchity komp'yuternykh setei: ekonomicheskie asprkti [Information security and computer network protection strategies: economics aspects]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 13 (9A), pp. 581-589. DOI: 10.34670/AR.2023.86.75.035

Keywords

Computer network, security technology, encryption, information technology, network security protocols.

References

1. Goldstein F.B., Goldstein B.S. (2005) *Tekhnologiya i protokoly MPLS* [Distributed Computer and Communication Networks]. St. Petersburg: BKhV-Peterburg Publ.
2. Gribunin V.G., Chudovskii V.V. (2009) *Kompleksnaya sistema informatsionnoi bezopasnosti na predpriyatii* [Comprehensive information security system at the enterprise]. Moscow: Akademiya Publ.
3. Kravets A.A., Kukartsev V.V., Senashov S.I. (2012) Organizatsiya informatsionnoi sistemy sbora dannykh po meditsinskoi pomoshchi na territorii kraya [Organization of an information system for collecting data on medical care in the region]. *Aktual'nye problemy aviatsii i kosmonavtiki* [Current problems of aviation and astronautics], 8, pp. 396-397.
4. Kukartsev V.V., Sheenok D.A. (2013) Optimizatsiya programmnoi arkhitektury logisticheskikh informatsionnykh sistem

[Optimization of the software architecture of logistics information systems]. *Logisticheskie sistemy v global'noi ekonomike* [Logistics systems in the global economy], 3, pp. 138-145.
5. Kulyagin V.A. et al. (2015) Kontseptual'naya model' mnogoetapnoi kompleksnoi otsenki nadezhnosti avtomatizirovannykh sistem upravleniya predpriyatiyami [Conceptual model of a multi-stage complex assessment of the reliability of automated enterprise management systems]. *Fundamental'nye issledovaniya* [Fundamental Research], 7-2, pp. 323-327.
6. Maksimov V. (2003) Mezhsetevye ekrany. Sposoby organizatsii zashchity [Firewalls. Methods of organizing protection]. *Komp'yuterpress* [Computerpress], 3, p. 68.
7. Olvein V. (2004) *Struktura i realizatsiya sovremennoi tekhnologii MPLS* [Structure and Implementation of Modern MPLS Technology]. Moscow: Vil'yams Publ.
8. Sergeev A.N. (2016) *Osnovy lokal'nykh vychislitel'nykh setei* [Fundamentals of local computer networks]. St. Petersburg: Lan' Publ.
9. Tanenbaum A. (2012) *Komp'yuternye seti* [Computer Networks]. St. Petersburg: Piter Publ.
10. Tynchenko V.S., Sakhaltueva Yu.S., Platonova O.V. (2016) Primenenie OLAP-tekhnologii v upravlenii predpriyatiem [Application of OLAP technologies in enterprise management]. *Ekonomika i sotsium* [Economy and Society], 12-3, pp. 86-88.