УДК 004.056 https://doi.org/10.51301/vest.su.2021.i5.08

Н.С. Баймулдина, А.Е.Батыргалиева*
Казахский национальный университет им.аль-Фараби, Алматы, Казахстан
*e-mail: batyrgalieva.aisaule@mail.ru

СОВРЕМЕННЫЕ ТЕХНОЛОГИИ ЗАЩИТЫ КОРПОРАТИВНЫХ СЕТЕЙ

Аннотация. В данной статье рассматриваются современные технологии защиты корпоративных сетей. Используя технологии защиты корпоративных сетей разработчики программного обеспечения могут гарантировать безопасность программного обеспечения там, где оно будет использоваться. Но есть атаки, для которых инженер сетевой системы должен иметь лучшие средства защиты.

Ключевые слова: интернет, протокол, шифрование, ключ, средства защиты, алгоритм шифрования.

Введение. Информационная безопасность в корпоративной сети является одной из основных задач, решаемых при построении информационной безопасности на предприятии. Для этого необходимо разделять сотрудникам доступ к информационным ресурсам и предотвращать несанкционированный доступ к данным внутри корпоративной сети, а также извне. При построении защиты используются программные решения в области информационной безопасности, которые позволяют настраивать политику безопасности предприятия, централизованно управлять процессами безопасности, интегрировать различные механизмы в единую систему и распределять разные роли для администрирования защищенной системы. Есть много способов атаки на корпоративную сеть. В процессе работы информационной системы риски сводятся к оптимальному значению потери таких основных свойств информации, как: целостность, конфиденциальность и доступность. В то же время риски остаются вне зависимости от эффективности используемой системы защиты.

В настоящее время практически вся информация хранится в цифровом виде. Цифровую информацию всегда легко, дешево и быстро скопировать. И большинство услуг включает в себя доступ через сеть. Это обязательно в большинстве случаев, как банкомат или система бронирования мест. Информация должна быть актуальной и доступной каждый раз, когда это необходимо. Это делает систему уязвимой. Поскольку Интернет-это открытая сеть, мы должны предполагать, что всегда есть кто-то, кто слушает, кто заинтересован в нашей информации. Мы должны использовать подходящий метод для обеспечения нашей конфиденциальности. Метод сильно зависит от случая. Нам нужно оценить, насколько важной информацией мы располагаем, и кто в ней заинтересован. Это самая важная информация при выборе метода защиты.

Эта область очень широка, и у разных компаний разные потребности в безопасности информационных систем. Банки и IT-компании разные, но и у тех, и у других много материала, который не может быть публичным. Тем не менее, деловой партнер может иметь доступ к этому материалу.

Онлайн-бизнес сам решает свои проблемы в этой среде. И просто иметь бизнес в Интернете. Им нужны совершенно новые, очень требовательные решения в области безопасности. Гораздо проще играть в ковбоя в Интернете, чем на обычном рынке. Все большая доля услуг может быть доступна в Интернете.

1. Средства защиты для сетей TCP/IP

Интернет состоит из множества сетей. Сеть нуждается в некоторых протоколах для передачи и приема данных. TCP/IP-это семейство протоколов, которое в настоящее время широко используется практически в каждой сетевой системе.

IP-это протокол без подключения. Это означает, что данный протокол не гарантирует правильную доставку данных. IP заботится о необходимой маршрутизации в Интернете. TCP-это протокол, ориентированный на соединение, и он обеспечивает доставку данных к получателю. Протокол TCP работает по протоколу IP. TCP/IP состоит из многих других субпротоколов, но в этом контексте нет необходимости понимать их все. TCP/IP-это просто способ передачи данных. Он не отвечает на вопросы безопасности. Поэтому необходимы специальные протоколы и способы обеспечения безопасности. И далее мы рассмотрим наиболее используемые и наиболее важные способы этого закрепления. [2]

1.1 SSL (Secure Socket Layer)

Это использование в WWW-среде (World Wide Web). Существуют 40-битные и 128-битные версии SSL - шифрования. Это широко используется в онлайновых банковских и рыночных системах. SSL-это протокол, созданный компанией Netscape Communications. Его цель - обеспечить конфиденциальность и целостность сообщений при использовании соединений TCP/IP. В онлайн банковской системе личная информация передается с использованием SLL - шифрования, но “безвредная” информация, то есть информация, не нуждающаяся в защите, не шифруется.

Протокол используется через TCP/IP и ниже HTTP или IMAP. Когда SSL используется, например, для обеспечения безопасности протоколов HTTP, HTTP-пакет инкапсулируется и шифруется в SSL - пакете, который инкапсулируется в TCP-пакете. 40-битная версия SSL-шифрования не может считаться безопасной, но, насколько мы знаем сейчас, 128-битная по-прежнему безопасна для общего использования. SSL-протокол состоит из множества подпротоколов, которые я здесь не привожу. Алгоритм шифрования в SSL может быть, например, DES, triple-DES или RC4. RC4-это алгоритм потокового шифрования, который используется в сетях GSM и беспроводной локальной сети. Существуют различные версии SSL; самые большие различия между ними заключаются в поддерживаемых алгоритмах шифрования и возможностях цифровой подписи. [3, 4, 5]

1.2 SSH (Secure SHell)

SSH изначально был создан Тату Илененом, финским сетевым ученым. SSH-это защищенный терминал-эмулятор. Он предназначен для замены небезопасного TELNET-соединения. Эти соединения очень небезопасны, и никто не должен предлагать какие - либо услуги по протоколу TELNET. SSH - это единственный выбор, который мы можем сделать, когда кто-то предлагает такие услуги удаленного доступа. SSH также обеспечивает надежное шифрование по разумной цене. Использование ssh-терминала очень просто, но туннелирование может быть сложным. И только некоторые SSH-клиенты даже поддерживают туннелирование портов. Кроме того, SSH может использовать различные алгоритмы шифрования, такие как IDEA, DES и triple-DES. С помощью SSH можно сделать безопасный туннель из точки в точку и передать в него любую TCP/IP связь. Таким образом, этот протокол подходит для самых разных видов использования. [6]

Например, внутренние передачи данных компании могут быть туннелированы через SSH. Например, взаимодействие между веб - сервером online markets и сервером клиентской базы данных. А когда у компании есть компьютеры в разных местах, удаленный доступ должен использовать SSH вместо TELNET. Например, в моей работе у нас есть огромное количество маршрутизаторов и коммутаторов, которыми мы управляем удаленно. Этот контроль должен использовать SSH, иначе информация может быть скомпрометирована.

1.3 PGP (Pretty Good Privacy)

PGP-это инструмент защиты, созданный Филиппом Циммерманом. Это должно сделать электронную коммуникацию более безопасной, и это действительно так, но PGP нелегко использовать. Первоначально он был предназначен только для частного использования. Но она быстро распространилась по всему миру через Интернет. PGP использует криптографию с открытым ключом для шифрования почты и других данных. Вам нужно знать открытый

ключ для шифрования. Но для расшифровки вам нужен закрытый ключ. Закрытый ключ не может быть скомпрометирован, потому что, если это произойдет, каждое сообщение также будет скомпрометировано. PGP использует два различных алгоритма шифрования. Сначала сообщение шифруется случайным образом выбранным ключом с использованием алгоритма шифрования IDEA. IDEA расшифровывается как Международный алгоритм шифрования. IDEA-это симметричная криптосистема, поэтому для шифрования и дешифрования используется один и тот же ключ. Затем ключ шифруется с помощью алгоритма RSA. И этот зашифрованный ключ IDEA вложен в сообщение.

Почему это делается так сложно? Ответ таков: IDEA-это гораздо более быстрый алгоритм, чем RSA. Если бы большой объем данных был зашифрован с помощью алгоритма RSA, это заняло бы много процессорного времени. Обе криптосистемы сильны, и это, при правильном дизайне, делает PGP сильным шифром. PGP не идеален, совсем нет. Проблема заключается в количестве открытых ключей (брелоков). Эта сумма может быстро расти, и ею трудно управлять. Даже в одной компании это может сделать этот метод совершенно невозможным. Именно по этой причине PGP до сих пор используется в основном частными лицами, а не компаниями. [7]

PGP может решить проблемы с безопасностью электронной почты компании. Но из-за управления ключами это не всегда идеальное решение.

1.4 IPSec (IP Security Protocol)

IPSec предназначен для обеспечения безопасности на сетевом уровне. IETF (Internet Engineering Task Force) координирует разработку. IPSec указан в RFC (Request For Comments) 1825-1829. IPSec может использоваться поверх IPv4 и является частью архитектуры IPv6. IPSec не определяет алгоритмы шифрования или аутентификации.

IPSec использует заголовок аутентификации (AH) для аутентификации и Инкапсулирующую полезную нагрузку безопасности (ESP) для безопасной передачи данных. Есть два способа использования ESP. Его можно использовать для туннелирования так, чтобы весь IP-пакет был зашифрован и инкапсулирован в IPSec - пакеты ESP-части кадра. Или просто часть данных IP-пакета может быть зашифрована и инкапсулирована. Они предназначены для различного рода использования.

Режим туннелирования может использоваться для соединения двух (или более) доверенных сетей через небезопасную сеть. Это делается двумя шлюзами, расположенными между доверенной сетью и небезопасной сетью, и туннелирующими весь трафик между ними.

Транспортный режим также может быть использован, но он не гарантирует полностью тот же уровень безопасности, что и режим туннелирования. Этот режим также может быть использован в сетевых решениях host-to-host и host-to-trusted. И компьютеры в доверенных сетях, конечно, могут использовать этот метод.

IPSec требует, чтобы отправитель и получатель могли совместно использовать свои открытые ключи. Существует специальный протокол, предназначенный для этого использования, называемый ISAKMP (Internet Security Association and Key Management Protocol).

Преимущества IPSec заключаются в прозрачности для верхних слоев. Использование IPSec не требует каких-либо изменений в приложениях. IPSec может быть включен в брандмауэры и архитектуру брандмауэра.

Недостатки заключаются в том, что на сетевом уровне различные потребности приложения в безопасности не могут быть разделены. И еще один недостаток заключается в том, что нет единого решения, которое могло бы быть решением всех проблем безопасности. [12, 13]

1.5 WEP (Wireless Encryption Protocol)

WEP-это стандарт шифрования в беспроводных Ethernet-решениях. WEP использует алгоритм шифрования RC4. WLAN (Беспроводная локальная сеть) использует 40-битное или 128-битное шифрование ключи. Эта криптосистема сильно критикуется, но ей по-прежнему доверяют большинство компаний. В августе 2001 года Флюрер, Мантин и Шамир опубликовали научную статью о слабых сторонах алгоритма планирования ключей RC4. В WEP-алгоритме есть ошибка, которая делает возможной очень опасную атаку. Можно скомпрометировать ключ шифрования, просто прослушав передачу. Эта атака полностью пассивна, и никто не может узнать, была ли эта атака сделана или кто-то просто делает эту атаку. WEP никоим образом не безопасен. Проблема не в алгоритме RC4, а в том, как WEP его использует. Компании обязательно должны иметь какие-то другие методы защиты интранета компании. Мое мнение заключается в том, что безопасность должна рассматриваться также на более высоких уровнях топологии сетевого протокола. Если мы примем на уровне TCP предположение, что все может быть прослушано, и разработаем безопасное программное обеспечение для этой среды, у нас будет хорошая основа для создания безопасной сетевой системы. Проблема WEP позволяет легко установить пиратский компьютер в интранет компании. Таким образом, брандмауэр не является решением этой проблемы. Если у компании есть очень секретная информация, компания не должна использовать беспроводную сеть или эта беспроводная сеть должна быть отдельно от интранета компании. [8, 9]

1.6 VPN (Virtual Private Network)

VPN-это метод безопасности, позволяющий подключать две (или более) частные сети через Интернет. Основная идея заключается в том, что VPN-маршрутизатор шифрует весь IP-пакет и отправляет его через Интернет. Это называется VPN-туннелем. Это намного дешевле, чем подключение по арендованной линии. И VPN может быть полностью прозрачным для приложений. Это самая важная идея VPN. VPN распространены, и их количество растет с каждым днем. Больше нет необходимости во всемирной сети компаний, основанной на арендованных линиях. VPN не говорит, какой протокол шифрования или метод аутентификации должен использоваться. VPN-это всего лишь требования для безопасного подключения двух (или более) сетей. [10]

2. Кое-что об используемых алгоритмах

Если нам нужна надежная конфиденциальная информация, нам нужна сильная криптография. Используя криптографию, мы можем блокировать распространение информации посторонним лицам, но в то же время можем передавать ее уполномоченным лицам. Криптография-это всего лишь инструмент, и если ее неправильно использовать, она не будет иметь никакого смысла. А поскольку приложения различны, существуют различные криптографические системы для различных нужд. Безопасность может быть обеспечена на разных уровнях сети. Но нет единого решения, которое подходило бы для всех. И нет ни одного слоя, который был бы более важен для защиты, чем любой другой.

Существует два вида шифрования: симметричное и асимметричное. В симметричной криптографии существует только один секретный ключ (“пароль”), который используется для шифрования и дешифрования. В криптографии с открытым ключом для этих целей используются два разных ключа. Технически шифры можно разделить на две категории: блочные и потоковые. Blockcipher нуждается в блоке, например, 64-битном образце для кодирования или декодирования. Потоковый шифр принимает бит за битом. Блочный шифр может менять, например, битовые места в некоторой последовательности. Потоковый шифр каждый бит находится в порядке, и шифрование базируется только на предыдущих битах и на ключе шифра. [1]

2.1 RSA (Rivest, Shamir, Adleman)

RSA-это криптосистема с открытым ключом, которая основана на том, что факторизация больших чисел является очень сложной операцией. Другими словами, когда умножаются два больших простых числа, почти невозможно получить эти два простых числа из результата. Этот "факт" не доказан математически, поэтому когда-нибудь кто-нибудь найдет для этого простой метод. Однако это крайне маловероятно. RSA хорошо известен и хорошо изучен, и он все еще хранится как сильный шифр. Недостатком является то, что алгоритм является математически тяжелым. Шифрование больших объемов данных происходит очень медленно. [1]

2.2 DES, 3DES (Data Encryption Standard)

Это может быть самая известная криптосистема. Этот алгоритм был разработан исследователями в IBM в 70-х годах. DES-это симметричный алгоритм шифрования, который означает, что один и тот же ключ используется при шифровании и дешифровании. АНБ прочно ассоциируется с DES. Когда IBM создавала DES, АНБ внесло некоторые изменения и никак не оспаривало их. Из-за этих причин некоторые скептики подозревают, что АНБ вставило бы "черный ход" в DES. Это облегчило бы прослушивание и контроль сообщений, которые шифруются с помощью DES. DES-это блочный шифр; данные шифруются в 64-битных длинных блоках. DES предназначен для аппаратного шифрования, но в настоящее время также используются программные решения, поскольку компьютеры гораздо быстрее, чем в 70-е годы. Но DES использует 56-битную длину ключа, которая абсолютно слишком коротка для безопасного использования. Даже домашние компьютеры могут совершить атаку грубой силы против DES в разумные сроки. 3DES-это решение этой проблемы; он использует три различных 56-битных ключа, которые так же безопасны, как и один 168-битный ключ. [1]

3. Другие методы, необходимые для обеспечения безопасности

3.1 Брандмауэр

Брандмауэр используется для предотвращения несанкционированного доступа к интрасети компании. Это очень важная часть политики безопасности компании. В настоящее время это самый важный способ защиты цифровой информации компаний. Брандмауэр фильтрует трафик, и входящие соединения могут быть ограничены или полностью ограничены. При этом весь необычный трафик хранится в лог-файлах для более детального анализа. Брандмауэр может быть настроен таким образом, чтобы партнеры по сотрудничеству и дочерние компании могли иметь доступ к интрасети. Брандмауэр физически располагается между собственной интрасетью компании и общедоступным Интернетом. Трафик между этими сетями проходит через брандмауэр. В большой компании или если компания имеет много другой информации, эти области могут быть разделены брандмауэрами.

4. SET (Secure Electronic Transaction)

SET - это решение для безопасной оплаты в Интернете, разработанное Visa и Mastercard. SET делает возможными безопасные платежи без значительных изменений в бизнес-системах. SET - это открытый стандарт, который широко поддерживается. Большинство компаний-разработчиков программного обеспечения и банков поддерживают этот стандарт. SET-стандарт нацелен на предоставление каждому участнику торговли безопасного способа оплаты. Совместимость также является ключевой проблемой. SET разработан с учетом того, что сеть небезопасна. Как я уже упоминал ранее, это хорошая основа для безопасной системы. SET был опубликован в июне 1997 года. SET может использоваться при оплате кредитной или банковской картой. На первом этапе принимаются только платежи по кредитной карте. SET выполняет все необходимые проверки подлинности и безопасности на уровне приложений. Так что он совместим с любой архитектурой. Это идеально. Но SET не так широко используется, по крайней мере, пока. [11]

5. Как использовать эти методы на практике?

5.1 Продовольственный магазин (пример)

Веб-магазин может быть реализован с использованием 128-битного SSL-шифрования. В этом случае платежи по кредитным картам, заказы и т. Д. Информация передается безопасным способом. Информация, которая предназначена только для внутреннего использования, должна быть защищена брандмауэром. Это ограничивает любую попытку получить доступ к этой информации. Если мы хотим разрешить доставку товаров для доступа к базе данных склада, это можно сделать, разрешив этот доступ только с определенных IP-адресов. И доступ разрешен только к этой базе данных. SET- это лучший способ оплаты. Это обеспечивает наилучшую совместимость и минимизирует инвестиции в устройство, а также не требует безопасности в сети, поскольку этот протокол сам по себе безопасен и предназначен для небезопасных сред. Таким образом, безопасность не требуется на более низких уровнях протокола.

На рис. 1 это представляло собой решение. На этом рисунке переданные данные защищены с помощью SSL-шифрования между онлайн-рынком и клиентом. Пунктирная линия описывает внутреннюю сеть компании. Эта сеть изолирована с помощью брандмауэров, и внешние соединения, как с клиентом, так и с банком, передаются через брандмауэр. Клиент использует также прямое соединение с банком, для этого используется SET протокол. Внутри компании сетевые программы используют алгоритм 3DES, чтобы гарантировать, что даже если кто - то имеет незаконный доступ к интранету компании, передаваемые секреты не находятся в опасности.

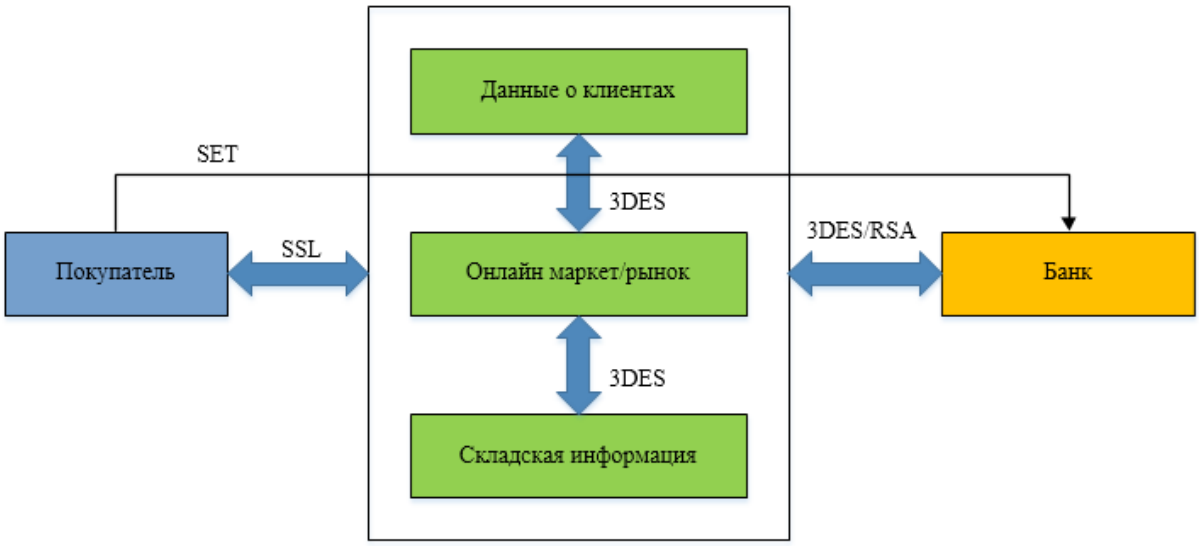

Рис. 1. Пример решения для онлайн-рынка

6. Как и кто выбирает правильный метод

Ответственность за разработку методов безопасности лежит на администрировании данных. Администрация данных должна назвать лицо, ответственное за поиск, и указать методы, необходимые для сохранения информации компании в тайне. Этот человек должен полагаться на свои собственные знания и при необходимости консультироваться с другими профессионалами. Политика безопасности должна быть принята директорами компании. Но каждый сотрудник должен взять на себя обязательство следовать политике безопасности. Если этого не сделать, то это документ без какого-либо практического использования. Но в каждой компании, независимо от размера, должна быть написана политика безопасности.

Политика безопасности включает в себя правила контроля доступа и принципы измерения уровня безопасности информации.

Выводы. Решения и инструменты безопасности должны использоваться на всех уровнях OSI. В лаборатории или в очень маленьком бизнесе мы могли бы выжить, обеспечив только прикладной уровень, но в гетерогенном реальном мире это невозможно. И что самое главное, разработчик программного обеспечения никогда не должен предполагать ничего (хорошего) о сетевой безопасности. И наоборот, инженер сетевой системы не должен ничего предполагать о безопасности приложения. Инженер сетевой системы не может гарантировать безопасность во всем Интернете, это факт. Но разработчик программного обеспечения может гарантировать безопасность программного обеспечения там, где оно будет использоваться. Нет абсолютно никакой идеи о повторном шифровании данных на всех уровнях протокола, что не дает никакой дополнительной безопасности. Но вопросы безопасности должны рассматриваться на всех уровнях. Все слои разные, и угрозы разные.

И техника-это еще не все. Дело в том, что их нужно использовать с умом. Компания нуждается в политике безопасности. И информация должна быть отсортирована по разным уровням безопасности. Доступ к контуру также является ключевым вопросом: кто, когда и где уполномочен получать доступ к этой информации? Об этом должно быть сказано в политике безопасности компании. И каждая компания тоже отличается, нет единого подходящего для всех решения, решения очень зависят от конкретного случая.

REFERENCES

[1] Bruce Scheier. *Applied Cryptography*. Wiley 1996.

[2] H. Gilbert. *Introduction to TCP/IP*, 2.2.1995, [referred 7.11.2001].

[3] Netscape Corporation. *Introduction to SSL*, 1998, [referred 15.10.2001].

[4] N.N.*Designing a Secured Website*, [referred 15.12.2001].

[5] Peter Robinson. *Understanding Digital Certificates and Secure Sockets Layer (SSL)*, January 2001, [referred 15.12.2001].

[6] Tatu Ylönen. SSH – *Secure Login Connections over the Internet*, March 1996, [referred 15.12.2001].

[7] J. Callas, L. Donnerhacke. *OpenPGP Message Format*, [referred 15.10.2001].

[8] Scott Fluhrer, Itsik Mantin, Adi Shamir. *Weaknesses in the Key Scheduling Algorithm of RC4*, [referred 15.10.2001].

[9] N.N. *Mobile LAN Secure Position*, [referred 15.12.2001].

[10] Egil Halvorsen, Rune Hansen. *IPSec based Virtual Private Networks (VPNs)*, [referred 15.12.2001].

[11] TIVIKE. *Elektronisen kaupankäynnin SET-ratkaisu*, June 2001, [referred 15.10.2001].

[12] Ghislaine Labouret. *IPsec: a technical overview*, June 16, 2000, [referred15.12.2001].

[13] N.N. *IP Security Protocol (ipsec)*, November 2, 2001, [referred 15.12.2001].

Н.С. Баймулдина, А.Е.Батыргалиева*
әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
*e-mail: batyrgalieva.aisaule@mail.ru

КОРПОРАТИВТІК ЖЕЛІЛЕРДІ ҚОРҒАУДЫҢ ЗАМАНАУИ ТЕХНОЛОГИЯЛАРЫ

Аңдатпа. Бұл мақалада корпоративтік желілерді қорғаудың заманауи технологиялары қарастырылады. Корпоративтік желілерді қорғау технологиясын қолдана отырып, бағдарламалық жасақтама жасаушылар бағдарламалық жасақтаманың қауіпсіздігін қамтамасыз ете алады. Бірақ желілік жүйенің инженері ең жақсы қорғаныс құралдарына ие болуы керек шабуылдар бар.

Негізгі сөздер: интернет, хаттама, шифрлау, кілт, қорғау құралдары, шифрлеу алгоритмі.

N.S. Baimuldina, A.Ye. Batyrgaliyeva*
al-Farabi Kazakh national university, Almaty, Kazakhstan
*e-mail: batyrgalieva.aisaule@mail.ru

MODERN TECHNOLOGIES FOR PROTECTING CORPORATE NETWORKS

Abstract. This article discusses modern technologies for protecting corporate networks. Using corporate network protection technologies, software developers can guarantee the security of software where it will be used. But there are attacks for which a network system engineer should have the best means of protection.

Keywords: internet, protocol, encryption, key, security tools, encryption algorithm.