БЕЗОПАСНОСТЬ ЦИФРОВЫХ ТЕХНОЛОГИЙ. – 2022. – № 3 (106). – 81–97

МЕТОДЫ И СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 004.056 DOI: 10.17212/2782-2230-2022-3-81-97

ТЕХНОЛОГИИ И МЕТОДЫ СОЗДАНИЯ СИСТЕМ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА*

И.Л. РЕВА[1], И.А. ОГНЕВ[2], А.А. ЯКИМЕНКО[3], О.К. АЛЬСОВА[4]

[1] 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент, декан факультета автоматики и вычислительной техники. E-mail: reva@corp.nstu.ru
[2] 630073, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, аспирант кафедры защиты информации. E-mail: i.ognev.2016@corp.nstu.ru
[3] 630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент, заведующий кафедрой вычислительной техники. E-mail: yakimenko@corp.nstu.ru
[4] 630073, РФ, г. Новосибирск, пр. Карла Маркса, 20, Новосибирский государственный технический университет, кандидат технических наук, доцент, доцент кафедры вычислительной техники. E-mail: alsova@corp.nstu.ru

В настоящей статье представлено описание существующих технологий и методов создания систем защищенного информационного обмена. На сегодняшний день системы защищенного информационного обмена строятся в соответствии с двумя технологиями (технология VPN и криптографические протоколы SSL или TLS), а также в соответствии с комбинациями данных технологий. Рассмотрена необходимость создания систем сетевой безопасности. Стремительное развитие сетевых технологий ведет за собой не менее бурный рост рисков информационной безопасности для компаний как государственного, так и частного сектора. Представлены требования законодательства Российской Федерации в сфере обеспечения безопасности сетей. Описаны принципы проектирования безопасности сетей. Проведен анализ существующих проектов и реализаций безопасности сетей. Приведено описание существующих методов построения систем защищенного информационного обмена. Рассмотрены технологии построения систем защищенного информационного обмена на основе технологии VPN, а также алгоритмы построения VPN-соединений – PPTP, IPSec, L2TP, SSTP, OpenVPN, ГОСТ VPN. Описаны наиболее распространенные технические и программные средства защиты информации, использующие VPN для построения защищенного информационного обмена – продукты компаний «ИнфоТеКС», «Код Безопасности», «С-Терра». Рассмотрена технология построения систем защищенного информационного обмена на основе криптографических протоколов SSL и TLS. В настоящей статье выявлены самые распространенные проблемы построения систем защищенного информационного обмена –

* Статья получена 10 августа 2022 г.

наличие большого количества производителей средств защиты информации со своей экосистемой, а также высокие трудовые, финансовые и временные затраты на обеспечение информационного обмена систем разного уровня защищенности, безопасность которых построена на решениях разных вендоров.

Ключевые слова: информационная безопасность, информационный обмен, защищенный информационный обмен, VPN, безопасность сетей, защищенные сети, протоколы, криптографические протоколы

ВВЕДЕНИЕ

В настоящее время организационные компьютерные сети становятся большими и повсеместными. Предполагая, что у каждого сотрудника есть выделенная рабочая станция, в крупной компании будет несколько тысяч рабочих станций и много серверов в сети.

Вполне вероятно, что эти рабочие станции не могут управляться централизованно и не имеют защиты по периметру. Они могут иметь различные операционные системы, аппаратные средства, программное обеспечение и протоколы с разным уровнем киберосведомленности среди пользователей. А теперь представьте, что эти тысячи рабочих станций в сети компании напрямую подключены к Интернету. Этот вид незащищенной сети становится целью для атаки, которая содержит ценную информацию и отображает уязвимости.

Сетевая безопасность охватывает множество компьютерных сетей, как государственных, так и частных, которые используются в повседневной работе, проводя транзакции и коммуникации между предприятиями, государственными учреждениями и частными лицами. Сети могут быть частными (например, внутри компании) и иными (которые могут быть открыты для доступа общественности).

1. ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА РФ В СФЕРЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СЕТЕЙ

Информатизация различных отраслей экономики Российской Федерации ведет к введению требований регуляторов по защите каналов связи с применением средств криптографической защиты информации.

1. В финансовой сфере действуют:

– положение Банка России № 672-П [1] «О требованиях к защите информации в платежной системе Банка России»;

– ГОСТ Р 57580.1–2017 [2], базовый стандарт для страховых организаций по проведению операций на финансовом рынке.

– предписание Банка России и ПАО «Ростелеком» № 4859-У/01.01.782-18 [3], которое требует обеспечения криптозащиты на всех этапах передачи данных между инфраструктурами банков и услугами электронного правительства.

2. В сфере здравоохранения Минздравом РФ издан Приказ № 911н [4], который требует использования сертифицированных средств защиты, в том числе для каналов связи, и который распространяется на все медицинские и фармацевтические организации.

3. В электроэнергетике в конце 2018 года утвержден приказ Минэнерго № 1015 [5], согласно которому для защиты систем дистанционного контроля и диагностики (СУМиД) должны применяться сертифицированные средства защиты.

4. В сфере обработки персональных данных использование сертифицированных средств криптографической защиты операторами персональных данных регулируется:

– Постановлением Правительства № 1119 [6];

– Приказом ФСБ России № 378 [7].

5. Подключение организаций к центрам мониторинга в соответствии с приказом ФСБ России №196 [8] требует использования сертифицированных средств криптографической защиты информации.

6. Для прохождения аттестации, которую проводит ФСБ России, средства криптографический защиты информации должны использовать отечественные криптографические алгоритмы (ГОСТ 34.12–2018 [9], ГОСТ 34.13–2018 [10]).

При создании виртуальных частных сетей частные организации могут использовать любые криптографические алгоритмы – как зарубежные, так и отечественные. Но при этом следует иметь в виду, что зарубежные криптографические алгоритмы не сертифицированы ФСБ России. Поэтому для соответствия требованиям регуляторов в некоторых случаях необходимо использовать средства криптографической защиты информации с отечественными криптографическими алгоритмами.

2. ОПИСАНИЕ ТЕХНОЛОГИЙ И МЕТОДОВ ПРОЕКТИРОВАНИЯ БЕЗОПАСНОСТИ СЕТЕЙ

2.1. ПРИНЦИПЫ ПОСТРОЕНИЯ БЕЗОПАСНОСТИ СЕТЕЙ

Цели создания безопасных сетей заключаются в обеспечении функционирования таких потоков информации, которые улучшают бизнес-процессы организации, и предотвращении потоков информации, которые их ухудша-

ют [11]. Подготовительные работы по проектированию и реализации безопасности сетей включают в себя следующие этапы:

– идентификация активов;
– сбор требований;
– анализ требований;
– оценка технических возможностей и ограничений;
– оценка существующих проектов и реализаций.

Идентификация активов – важный первый шаг в выявлении рисков информационной безопасности всех сетей. Защищенные активы – это активы, которые могут ухудшить бизнес-процессы организации, если их целостность, доступность и конфиденциальность будут нарушены. К ним относятся физические активы (серверы, коммутаторы, маршрутизаторы и т. д.) и логические активы (параметры конфигурации, исполняемый код, данные и т. д.). Этот список активов должен быть создан в рамках планирования непрерывности бизнеса и анализа рисков аварийного восстановления.

К идентифицируемым активам относятся активы, необходимые для безопасной поддержки процессов управления пользовательским трафиком и контроля, а также функции, необходимые для работы сетевой инфраструктуры, сервисов и приложений. К ним относятся такие устройства, как хосты, маршрутизаторы, брандмауэры и т. д., интерфейсы (внутренние и внешние), хранимая/обрабатываемая информация и используемые протоколы. Защита активов инфраструктуры – это только часть цели проектирования сетевой безопасности. Основной целью является защита активов организации, таких как информация и бизнес-процессы.

Для построения безопасной сети необходимо проанализировать текущие возможности и все запланированные технические изменения в сетевой архитектуре и сравнить их с разрабатываемой технической архитектурой безопасности для выявления любых несоответствий. Все несоответствия должны быть проанализированы, а изменения внесены в соответствующие архитектуры.

Информация, которая должна быть получена в ходе анализа, должна включать как минимум следующее [11]:

– идентификацию типа (типов) сетевого соединения, которое будет использоваться;
– определение рисков безопасности;
– сетевые протоколы, которые будут использоваться;
– сетевые приложения, используемые в сети для различных целей.

Собранная информация должна быть представлена в контексте возможностей сети. Следует собрать и проанализировать подробную информацию о соответствующей сетевой архитектуре, чтобы сформировать необходимое понимание и содержание для последующих этапов процесса.

Рассмотрение аспектов архитектуры сети и приложений на ранней стадии даст время для анализа этих архитектур и. Это даст возможность пересмотреть их, если приемлемое решение безопасности не может быть реально получено с текущей архитектурой.

Анализ существующих мер безопасности следует проводить в рамках соответствующего этапа управления рисками безопасности и анализа процессов управления рисками безопасности [11]. Результаты оценки рисков безопасности могут указать, какие меры безопасности необходимы для оцениваемых угроз. Чтобы определить, что не учитывается в существующей архитектуре сетевой безопасности, необходимо провести для нее анализ несоответствий.

2.2. АНАЛИЗ СУЩЕСТВУЮЩИХ ПРОЕКТОВ И РЕАЛИЗАЦИЙ БЕЗОПАСНОСТИ СЕТЕЙ

Архитектура сетевой безопасности должна учитывать все существующие меры безопасности, а также любые неиспользуемые или планируемые меры безопасности.

Архитектура сетевой безопасности предназначена для ограничения трафика, проходящего между разными доверенными доменами. Наиболее очевидная граница между доверенными доменами – это интерфейс между внутренней сетью организации и внешним миром. Организация, независимо от размера, также будет иметь границы между внутренними доменами доверия, которые необходимо идентифицировать и контролировать. Архитектура сетевой безопасности включает описание интерфейсов между внутренней сетью организации/сообщества и внешним миром.

Архитектура безопасности построена на следующих принципах:

- обеспечение многоуровневой защиты – использование нескольких мер обеспечения безопасности или методов защиты, которые позволяют снизить риск для каждого объекта защиты до того, как он будет скомпрометирован или выведен из строя;
- сегментирование сети – концепция, согласно которой системным ресурсам с разными значениями устойчивости к риску и восприимчивости к угрозам следует находиться в разных доменах безопасности;
- обеспечение отказоустойчивости системы безопасности сети. Проект безопасности сетей должен включать разумную избыточность средств защиты, чтобы исключить единые точки отказа и максимизировать доступность сетевой инфраструктуры;
- определение актуальных сценариев угроз безопасности. Такая информация очень полезна при рассмотрении вариантов архитектуры технической безопасности/проекта, а также при выборе и документировании предпочти-

тельного варианта архитектуры технической безопасности/проекта и соответствующих мер обеспечения безопасности;

- разработка модели и структуры безопасности сетей. Модель безопасности используется для описания сущностей (субъектов, регулируемых политикой безопасности организации) и определяет правила доступа, необходимые для реализации указанной политики; Структуры безопасности обычно способствуют организации в составлении общего представления о том, как сформировать защищенную систему.

3. ОПИСАНИЕ СУЩЕСТВУЮЩИХ ТЕХНОЛОГИЙ И МЕТОДОВ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА

3.1. ТЕХНОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА НА ОСНОВЕ VPN

Сегодня безопасный обмен информацией основан на построении сетей с использованием технологии VPN (Virtual Protected Network). VPN – это совокупность локальных сетей и отдельных компьютеров, объединенных в единую виртуальную защищенную сеть с целью обеспечения конфиденциальности, целостности и подлинности информации.

Виртуальные частные сети быстро развивались как средство взаимодействия и способ подключения удаленных пользователей к сетям.

Существует множество определений VPN. В своей простейшей форме они обеспечивают механизм для установления безопасного канала или каналов передачи данных по существующей сети или через соединение «точка – точка». Эти каналы доступны ограниченному числу пользователей и могут динамически устанавливаться и удаляться по мере необходимости. Сеть хостинга может быть как частной, так и публичной.

Удаленный доступ с использованием VPN реализуется через обычное двухточечное соединение. В первую очередь устанавливается стандартное двухточечное соединение между локальным пользователем и удаленными узлами. Некоторые виртуальные частные сети предоставляются как управляемая служба, обеспечивающая безопасный и надежный путь передачи данных по общедоступной инфраструктуре, а также управление и адресацию, эквивалентные тем, которые предоставляются в частной сети. Следовательно, для усиления безопасности VPN может потребоваться принятие во внимание дополнительных мер безопасности, как указано в этом стандарте.

Данные и код, передаваемые через VPN, должны предназначаться только для организации, использующей VPN, и храниться отдельно от данных и кода других пользователей базовой сети. Данные и код, принадлежащие другим пользователям, не должны передаваться по одному и тому же каналу VPN. При оценке объема дополнительных мер информационной безопасности, которые могут потребоваться, следует учитывать уровень уверенности в конфиденциальности и других аспектах безопасности организации, владеющей или предоставляющей VPN.

3.2. АЛГОРИТМЫ ПОСТРОЕНИЯ VPN-СОЕДИНЕНИЙ

PPTP [12] (Point-to-Point Tunneling Protocol). Основная направленность протокола – инкапсуляция пакетов протокола PPP в пакеты протокола IP и передача получившихся пакетов по сетям IP, в том числе и по Интернету.

IPsec (IP Security) [13] – это группа протоколов, реализующих безопасную передачу информации при передаче пакетов протокола IP. IPSec обеспечивает:

– конфиденциальность данных, передаваемых по IP-сетям;

– проверку подлинности и целостности передаваемой информации;

– шифрование передаваемых пакетов.

L2TP [14] (Layer 2 Tunneling Protocol) – это протокол туннелирования уровня 2 (канального уровня). Главное достоинство L2TP состоит в том, что этот протокол позволяет создавать туннель не только в сетях IP, но и в таких как ATM, X.25 и Frame Relay. Протокол позволяет организовывать VPN с заданными приоритетами доступа, однако не содержит в себе средств для защиты данных и механизмов аутентификации. Для этой задачи обычно используется IPsec [15].

SSTP [16] (Secure Socket Tunneling Protocol) – еще один продукт компании Microsoft, представленный с выпуском Windows Vista. Благодаря поддержке SSL v.3 протокол SSTP может работать без настройки маршрутизатора/брандмауэра, а Windows в комплекте обеспечивает стабильную работу.

OpenVPN [17] – относительно молодая (2002 год) реализация VPN с открытым исходным кодом, распространяемая под лицензией GNU GPL. Безопасность активных туннелей контролируется библиотекой OpenSSL, которая предлагает набор открытых инструментов (Blowfish, AES, Camelia, 3DES, CAST и т. д.).

ГОСТ VPN [9, 10] – сервис шифрования каналов связи на основе СКЗИ, сертифицированный ФСБ России. В рамках услуги ГОСТ ВПН используются СКЗИ, сертифицированные ФСБ России по классу КС3. Этот класс наиболее распространен и фактически является стандартом на российском рынке.

3.3. ОПИСАНИЕ ТЕХНИЧЕСКИХ И ПРОГРАММНЫХ СРЕДСТВ

ViPNet [18] создан для того, чтобы шифровать информацию, а также передавать ее по защищенным каналам связи, используя VPN. Соответствует стандарту ГОСТ 28147–89. Программно-аппаратный комплекс позволяет организовать защищенный доступ как в центре обработки данных, так и в корпоративной инфраструктуре.

Особенности ViPNet:

– при создании VPN применяется свой протокол ViPNet VPN. Он не зависит от вида канала связи и обеспечивает защищенное соединение;

– скорость шифрования 5,5 Гбит/с;

– отказоустойчивый;

– работает на разных ОС (например, Windows, macOS, Android, iOS, Linux).

Аппаратно-программный комплекс шифрования «Континент» (АПКШ) [19] создан отечественной фирмой «Код Безопасности». «Континент» гарантирует криптографическую защиту данных, передаваемых по открытых каналу. АПКШ соответствует ГОСТ 28147–89, а также дает возможность гарантировать защиту трафика в сетях, разбивать сегменты сети, реализовать защищенный удаленный доступ, осуществлять межсетевую связь с остальными защищенными сетями, сделанными на основе такого же продукта. «Континент» работает на основе FreeBSD.

Особенности АПКШ «Континент»:

– централизованное управление;

– централизованный мониторинг;

– резервирование настроек;

– скорость шифрования до 3,5 гбит/с;

– большое количество возможных интерфейсов.

– фильтр трафика;

– фильтр протоколов;

– фильтрация на базе статических списков.

Продукты «С-Терра» производства российской компании «С-Терра СиЭсПи» [20] поддерживают встроенную криптографическую библиотеку «С-Терра ST» (собственная разработка производителя), реализующую криптоалгоритмы на основе ГОСТ Р 34.10–2012, ГОСТ Р 34.11–2012, ГОСТ Р 34.12–2015, ГОСТ Р 34.13–2015 и совместимую с «Крипто-Про CSP». Таким образом, «С-Терра» может взаимодействовать с другими продуктами «С-Терра СиЭсПи» («С-Терра Шлюз», «С-Терра Клиент») и поддерживать совместимость с оборудованием других производителей, использующим IPsec (IKEv1) с тем же набором алгоритмов.

«С-Терра» – универсальное средство криптографической защиты информации, передаваемой по открытым каналам связи, беспроводным и мобильным сетям, с функциями межсетевого экранирования.

Основные функциональные возможности «С-Терра»:

– создание защищенных каналов связи с максимальной производительностью 10 Мбит/с по иностранным криптоалгоритмам и алгоритмам ГОСТ;

– защита интерфейсов управления (iLO, CIMC, IPMI);

– защита трафика на уровне аутентификации / шифрования сетевых пакетов по протоколам IKE / IPsec;

– пакетная фильтрация трафика по адресам, протоколам, портам, по любым полям заголовка IP-пакета и по расписанию;

– контекстная фильтрация трафика для протоколов TCP и FTP;

– формирование наборов правил на разных интерфейсах, а также для входящего и исходящего трафика;

– поддержка качества обслуживания QoS (приоритет по полю TOS; управление очередями, фрагментацией пакетов, сеансами TCP; классификация, защита от перегрузки);

– журналирование событий с возможностью их объединения в группы; сбор статистики для мониторинга по протоколу SNMP.

3.4. ТЕХНОЛОГИЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА НА ОСНОВЕ КРИПТОГРАФИЧЕСКИХ ПРОТОКОЛОВ

Криптографический протокол [21] – это абстрактный или конкретный протокол, включающий набор криптографических алгоритмов, часто последовательность криптографических примитивов. В основе протокола лежит свод правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах обмена сообщениями между двумя и более участниками, а также описание используемых структур.

В протоколе участниками (субъектом, стороной) могут быть приложения, люди, их группы или, например, организации. Другими словами, всё, что по тем или иным причинам способно играть активную или пассивную роль в работе протокола. Так, в частности, большинство протоколов разрабатываются с учетом наличия пассивного слушателя, способного перехватывать сообщения.

Криптографический протокол выполняет следующие функции [22]:

– генерация ключей;

– обмен ключами;

– аутентификация сторон;

– доказательство целостности и происхождения данных (ЭЦП);
– разделение ключей;
– безопасные распределенные вычисления;
– обеспечение конфиденциальности данных;
– обеспечение невозможности отказа;
– обеспечение целостности данных;
– обеспечение целостности соединения;
– контроль доступа.

SSL (Secure Sockets Layer) и TLS (Transport Level Security) [23, 24] – криптографические протоколы, целью которых является организация защищенной передачи информации в компьютерной сети.

SSL [25] (англ. Secure Sockets Layer – уровень защищенных сокетов) – криптографический протокол, который предполагает более безопасное соединение.

Протокол SSL обеспечивает безопасную связь с помощью следующих двух элементов:
– аутентификация;
– шифрование.

TLS [26] (transport layer security – протокол безопасности транспортного уровня), как и его предшественник SSL (secure sockets layer – уровень защищенных сокетов), – криптографический протокол, обеспечивающий безопасную передачу данных между узлами в Интернете.

TLS и SSL используют асимметричное шифрование для аутентификации, симметричное шифрование для конфиденциальности и коды аутентификации сообщений для сохранения целостности сообщений.

Поскольку большинство коммуникационных протоколов можно использовать как с TLS/SSL, так и без них, при установлении соединения вы должны явно указать серверу, хочет ли клиент установить TLS. Один из способов добиться этого – использовать порт, на котором соединение всегда устанавливается с помощью TLS (например, 443 для HTTPS). Другой способ – использовать специальную команду серверу от клиента для переключения соединения на TLS (например, STARTTLS для почтовых протоколов).

ЗАКЛЮЧЕНИЕ

В настоящее время системы безопасного обмена информацией строятся двумя основными способами.

1. На основе виртуальных частных сетей (virtual private network) или виртуальных защищенных сетей (virtual protected network) – VPN. Основная задача VPN – построить виртуальную безопасную сеть поверх сетей любого уровня доверия, от сетей общего пользования до корпоративных.

Сегодня на рынке есть компании, которые предлагают свои решения в области защиты как всего периметра сети, так и отдельных устройств. Программно-аппаратные комплексы в виде криптошлюзов и программного обеспечения для стационарных и мобильных устройств способны реализовать различные технологии VPN.

2. На основе криптографических протоколов SSL или TLS. Основной задачей криптографических протоколов является построение защищенных соединений между субъектами информационного обмена (например, приложениями, людьми, их группами или, например, организациями и т. д.) в соответствии с заложенными в протоколы криптографическими алгоритмами.

Как правило, использование технологии VPN заложено в сертифицированных средствах защиты информации для обеспечения безопасности сетей, в которых обрабатывается информация ограниченного доступа – различного рода конфиденциальная информация и государственная тайна разного уровня, т. е. параметры сети и конечные пользователи защищены. Криптографические протоколы чаще всего используются для обеспечения секретности и конфиденциальности личной информации пользователей при работе с общедоступными информационно-телекоммуникационными сетями, такими как Интернет.

Проанализировав весь материал, можно выделить следующие тенденции в области построения безопасного обмена информацией:

– наполнение рынка достаточно большим количеством различных производителей программно-аппаратных и программных средств для построения безопасного обмена информацией, каждый из которых обеспечивает свою экосистему внутри защищенной сети;

– наличие определенной градации требований законодательства об обеспечении безопасности сетей в соответствии с установленным уровнем защищенности этой информации.

В связи с этим возникает ряд проблем при построении безопасного обмена информацией различных сетей.

1. Проблема построения защищенного обмена информацией между сетями, безопасность которых обеспечивается за счет использования решений разных производителей. Сегодня эта проблема решается путем приобретения дополнительных средств сетевой безопасности, что порождает повышенные финансовые затраты для организаций, а также увеличивает трудоемкость построения защищенных каналов связи.

2. Проблема построения защищенного обмена информацией между сетями с разным уровнем защищенности. Сегодня эта проблема решается путем «подтягивания» уровня сетевой защиты с более низким уровнем безопасности до уровня сетевой защиты с более высоким уровнем безопасности, что по-

рождает ненужные финансовые затраты на приобретение средств сетевой безопасности для более высоких уровней безопасности, а также создает лишние трудо- и времязатраты на интеграцию новых средств защиты.

СПИСОК ЛИТЕРАТУРЫ

1. Положение Банка России № 672-П «О требованиях к защите информации в платежной системе Банка России».

2. ГОСТ Р 57580.1–2017. Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер. – М.: Стандартинформ, 2017. – 61 с.

3. Указание Банка России и ПАО «Ростелеком» № 4859-У/01/01/782-18 «О единой биометрической системе (ЕБС)».

4. Приказ Минздрава РФ от 24.12.2018 № 911н «Об утверждении Требований к государственным информационным системам в сфере здравоохранения субъектов Российской Федерации, медицинским информационным системам медицинских организаций и информационным системам фармацевтических организаций».

5. Приказ Министерства энергетики РФ от 06.11.2018 № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного мониторинга и диагностики энергетического оборудования».

6. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

7. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

8. Приказ ФСБ России от 06.05.2019 № 196 «Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты».

9. ГОСТ 34.12–2018. Информационная технология. Криптографическая защита информации. Блочные шифры. – М.: Стандартинформ, 2018. – 12 с.

10. ГОСТ 34.13–2018. Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров. – М.: Стандартинформ, 2018. – 23 с.

11. ГОСТ Р ИСО/МЭК 27033-2–2021. Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей. Ч. 2. Рекомендации по проектированию и реализации безопасности сетей. – М.: Стандартинформ, 2021. – 23 с.

12. RFC 2637. Point-to-Point Tunneling Protocol (PPTP).

13. RFC 4301. Security Architecture for the Internet Protocol.

14. RFC 2661. Layer Two Tunneling Protocol "L2TP".

15. RFC 3193. Securing L2TP using IPsec.

16. [MS-SSTP]: Secure Socket Tunneling Protocol (SSTP).

17. OpenVPN: Documentation. – URL: https://openvpn.net/vpn-server-resources/ (accessed: 30.08.2022).

18. ИнфоТеКС: Продуктовые линейки ViPNet. – URL: https://infotecs.ru/product/ (дата обращения: 30.08.2022).

19. Код безопасности: web-сайт. – URL: https://www.securitycode.ru (дата обращения: 30.08.2022).

20. С-Терра СиЭсПи: Продуктовая линейка. – URL: https://www.s-terra.ru/products/catalog/index.php (дата обращения: 30.08.2022).

21. *Menezes A.J., Oorschot P.C. van, Vanstone S.A.* Handbook of applied cryptography. – Boca Raton: CRC Press, 1996. – 816 p.

22. *Черемушкин А.В.* Криптографические протоколы: основные свойства и уязвимости // Прикладная дискретная математика: Приложение. – 2009. – № 2. – С. 115–150.

23. *Rescorla E.* SSL and TLS: designing and building secure systems. – Boston: Addison-Wesley, 2000. – 499 p.

24. *Thomas S.A.* SSL & TLS essentials: securing the Web. – New York: Wiley, 2000. – 197 p.

25. *Dierks T.* The Secure Sockets Layer (SSL). – RTFM, Inc., 2008.

26. *Dierks T., Rescorla E.* The Transport Layer Security (TLS) Protocol. Version 1.2. – RTFM, Inc., 2008. – 104 p.

Рева Иван Леонидович, кандидат технических наук, доцент, декан факультета автоматики и вычислительной техники Новосибирского государственного технического университета. Область научных интересов – информационная безопасность. E-mail: reva@corp.nstu.ru.

Огнев Игорь Александрович, аспирант кафедры защиты информации Новосибирского государственного технического университета. Основное

направление научных исследований – обеспечение безопасности информационных взаимодействий. E-mail: i.ognev.2016@corp.nstu.ru

Якименко Александр Александрович, кандидат технических наук, доцент, заведующий кафедрой вычислительной техники Новосибирского государственного технического университета. Основное направление научных исследований – математическое моделирование численных процессов, параллельные вычисления. E-mail: yakimenko@corp.nstu.ru

Альсова Ольга Константиновна, кандидат технических наук, доцент, доцент кафедры вычислительной техники Новосибирского государственного технического университета. Область научных интересов – математическое моделирование, имитационное моделирование, прогнозирование, машинное обучение. E-mail: alsova@corp.nstu.ru

DOI: 10.17212/2782-2230-2022-3-81-97

Technologies and methods for creating systems of secure information exchange*

I.L. Reva[1], I.A. Ognev[2], A.A. Yakimenko[3], O.K. Alsova[4]

[1] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, PhD in Technology, Associate Professor, Dean of the Faculty of Automation and Computer Engineering. E-mail: reva@corp.nstu.ru*

[2] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, graduate student of Information Security Department. E-mail: i.ognev.2016@corp.nstu.ru*

[3] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, PhD in Technology, Associate Professor, Head of the Department of Computer Science. E-mail: yakimenko@corp.nstu.ru*

[4] *Novosibirsk State Technical University, 20 Karl Marx Prospekt, Novosibirsk, 630073, Russian Federation, PhD in Technology, Associate Professor of the Department of Computer Science. E-mail: alsova@corp.nstu.ru*

This article presents a description of existing technologies and methods for creating secure information exchange systems. To date, secure information exchange systems are built in accordance with two technologies – VPN technology and cryptographic protocols SSL and TSL, as well as in accordance with combinations of these technologies. The necessity of creating network security systems is considered. The rapid development of network technologies leads to an equally rapid increase in information security risks for companies in both the public and private sectors. The requirements of the legislation of the Russian Federation in the field of ensuring the security of networks are presented. The principles of network security design are

* *Received 10 August 2022.*

described. The analysis of existing projects and implementations of network security was carried out. A description of the existing and methods for constructing secure information exchange systems is given. The technologies for building secure information exchange systems based on VPN technology, as well as the algorithms for building VPN connections - PPTP, IPSec, L2TP, SSTP, OpenVPN, GOST VPN are considered. The most common technical and software information security tools that use VPN to build a secure information exchange are described - the products of the companies InfoTeKS, Security Code, S-Terra. The technology of constructing secure information exchange systems based on SSL and TLS cryptographic protocols is considered. This article identifies the most common problems in building secure information exchange systems – the presence of a large number of manufacturers of information security tools with their own ecosystem, as well as high labor, financial and time costs for ensuring the information exchange of systems of different levels of security, the security of which built on solutions from different vendors.

Keywords: information security, information exchange, secure information exchange, VPN, network security, secure networks, protocols, cryptographic protocols

REFERENCES

1. Position of the Bank of Russia No. 672-P "On the requirements for information protection in the payment system of the Bank of Russia". (In Russian).

2. State standard R 57580.1–2017. *Security of financial (banking) operations. Information protection of financial organizations. Basic set of organizational and technical measures*. Moscow, Standartinform Publ., 2017. 61 p. (In Russian).

3. Ordinance of the Bank of Russia and PJSC Rostelecom No. 4859-U/01/01/782-18 On the Unified Biometric System (UBS). (In Russian).

4. Order of the Ministry of Health of the Russian Federation of December 24, 2018 No. 911n “On approval of the Requirements for state information systems in the field of healthcare of the subjects of the Russian Federation, medical information systems of medical organizations and information systems of pharmaceutical organizations”. (In Russian).

5. Order of the Ministry of Energy of the Russian Federation dated November 6, 2018 No. 1015 "On approval of requirements for basic (mandatory) functions and information security of electric power facilities during the creation and subsequent operation of remote monitoring and diagnostic systems on the territory of the Russian Federation power equipment". (In Russian).

6. Decree of the Government of the Russian Federation of 01.11.2012 No. 1119 “On approval of the requirements for the protection of personal data during their processing in personal data information systems”. (In Russian).

7. Order of the FSB of Russia dated July 10, 2014 No. 378 "On approval of the Composition and content of organizational and technical measures to ensure the security of personal data when they are processed in personal data information sys-

tems using cryptographic information protection tools necessary to comply with those established by the Government of the Russian Federation requirements for the protection of personal data for each of the levels of security". (In Russian).

8. Order of the FSB of Russia dated May 6, 2019 No. 196 "On Approval of the Requirements for Tools Designed to Detect, Prevent and Eliminate the Consequences of Computer Attacks and Response to Computer Incidents". (In Russian).

9. State standard 34.12–2018. *Information technology. Cryptographic data security. Block ciphers*. Moscow, Standartinform Publ., 2018. 12 p. (In Russian).

10. State standard 34.13–2018. *Information technology. Cryptographic data security. Modes of operation for block ciphers*. Moscow, Standartinform Publ., 2018. 23 p. (In Russian).

11. State standard R ISO/IEC 27033-2–2021. *Information technology. Security techniques. Network security.* Pt. 2. *Guidelines for the design and implementation of network security*. Moscow, Standartinform Publ., 2021. 23 p. (In Russian).

12. RFC 2637. *Point-to-Point Tunneling Protocol (PPTP)*.

13. RFC 4301. *Security Architecture for the Internet Protocol*.

14. RFC 2661. *Layer Two Tunneling Protocol "L2TP"*.

15. RFC 3193. *Securing L2TP using IPsec*.

16. [MS-SSTP]: Secure Socket Tunneling Protocol (SSTP).

17. OpenVPN: Documentation. Available at: https://openvpn.net/vpn-server-resources/ (accessed 30.08.2022).

18. InfoTeKS: ViPNet product lines. (In Russian). Available at: https://infotecs.ru/product/ (accessed 30.08.2022).

19. Security code: website. (In Russian). Available at: https://www.securitycode.ru (accessed 30.08.2022).

20. S-Terra CSP: Product line. (In Russian). Available at: URL: https://www.s-terra.ru/products/catalog/index.php ((accessed 30.08.2022).

21. Menezes A.J., Oorschot P.C. van, Vanstone S.A. *Handbook of applied cryptography*. Boca Raton, CRC Press, 1996. 816 p.

22. Cheremushkin A.V. Kriptograficheskie protokoly: osnovnye svoistva i uyazvimosti [Cryptographic protocols: basic properties and vulnerabilities]. *Prikladnaia diskretnaia matematika: Prilozhenie = Applied discrete mathematics. Application*, 2009, no. 2, pp. 115–150.

23. Rescorla E. *SSL and TLS: designing and building secure systems*. Boston, Addison-Wesley, 2000. 499 p.

24. Thomas S.A. *SSL & TLS essentials: securing the Web*. New York, Wiley, 2000. 197 p.

25. Dierks T. *The Secure Sockets Layer (SSL)*. RTFM, 2008.

26. Dierks T., Rescorla E. *The Transport Layer Security (TLS) Protocol. Version 1.2*. RTFM, Inc., 2008. 104 p.

Для цитирования:

Технологии и методы создания систем защищенного информационного обмена / И.Л. Рева, И.А. Огнев, А.А. Якименко, О.К. Альсова // Безопасность цифровых технологий. – 2022. – № 3 (106). – С. 81–97. – DOI: 10.17212/2782-2230-2022-3-81-97.

For citation:

Reva I.L., Ognev I.A., Yakimenko A.A., Alsova O.K. Tekhnologii i metody sozdaniya sistem zashchishchennogo informatsionnogo obmena [Technologies and methods for creating systems of secure information exchange]. *Bezopasnost' tsifrovykh tekhnologii = Digital Technology Security*, 2022, no. 3 (106), pp. 81–97. DOI: 10.17212/2782-2230-2022-3-81-97.