УДК 621.3

АСПЕКТЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ

Луцкий А.В.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Пискун Г.А. – к.т.н, доцент, доцент кафедры ПИКС

Аннотация. Показана, что обеспечение безопасности телекоммуникаций имеет решающее значение для обеспечения целостности, конфиденциальности и доступности сетей связи и данных. Рассмотрены различные аспекты защиты различных компонентов телекоммуникационной инфраструктуры, включая сетевые устройства, серверы, базы данных, протоколы связи и устройства конечных пользователей.

Ключевые слова: безопасность, телекоммуникационные системы, несанкционированный доступ, уровни безопасности.

Введение. Телекоммуникационные системы (ТКС) являются основой информационного общества. В современном взаимосвязанном мире безопасность телекоммуникаций имеет решающее значение для обеспечения целостности, конфиденциальности и доступности сетей связи и данных. В условиях растущей зависимости от телекоммуникаций в различных аспектах нашей жизни, включая личное общение, деловые операции и критически важную инфраструктуру, крайне важно понимать важность безопасности телекоммуникаций и связанные с ней проблемы [1−3].

Безопасность телекоммуникаций относится к мерам по защите телекоммуникационных сетей (ТКС), систем и данных от несанкционированного доступа, неправильного использования, сбоев или перехвата. Она охватывает широкий спектр технологий, протоколов, политик и процедур, предназначенных для защиты конфиденциальности, целостности и доступности каналов связи, а также информации, передаваемой через них.

Безопасность телекоммуникаций включает защиту различных компонентов телекоммуникационной инфраструктуры, включая сетевые устройства, серверы, базы данных, протоколы связи и устройства конечных пользователей. Сюда также входит обеспечение безопасности беспроводных сетей, мобильной связи и новых технологий, таких как 5G и Интернет вещей (*IoT*).

Основная часть. Индустрия связи способствовала повышению производительности и связующим звеньям сообществ во всем мире почти во всех промышленных сегментах. Такая эффективность коммуникационной инфраструктуры в немалой степени обусловлена стандартами, разработанными сектором стандартизации электросвязи Международного союза электросвязи (*ITU-T*). Стандарты, которые поддерживают эффективность существующих сетей, закладывают основу для сетей следующего поколения. Однако несмотря на то, что стандарты продолжают удовлетворять потребности конечных пользователей и отрасли, более широкое использование открытых интерфейсов и протоколов, множество новых участников, огромное разнообразие приложений и платформ, а также реализации, которые не всегда достаточно проверены, увеличивают возможности для злонамеренного использования сетей. В последние годы во всех глобальных сетях наблюдался всплеск нарушений безопасности (таких как вирусы и нарушение конфиденциальности хранимых данных), что часто приводило к серьезным финансовым последствиям. По этой причине вопрос о том, как поддерживать открытую коммуникационную инфраструктуру, не ставя под угрозу информацию, которой она обменивается, является актуальным.

Рекомендация X.805, разработанная *ITU-T*, определяет структуру архитектуры и параметры достижения сквозной безопасности распределенных приложений. Общие принципы и определения применимы ко всем приложениям, хотя такие детали, как угрозы и уязвимости, а также меры по противодействию или предотвращению, различаются в зависимости от потребностей приложения.

Архитектура безопасности определяется с точки зрения двух основных концепций: уровней и плоскостей. Уровни безопасности соответствуют требованиям, применимым к сетевым элементам и системам, составляющим сквозную сеть. При разделении требований по уровням используется иерархический подход, так что сквозная безопасность достигается за счет построения каждого уровня. Три уровня − это уровень инфраструктуры, уровень услуг и уровень приложений (рисунок 1) [1].

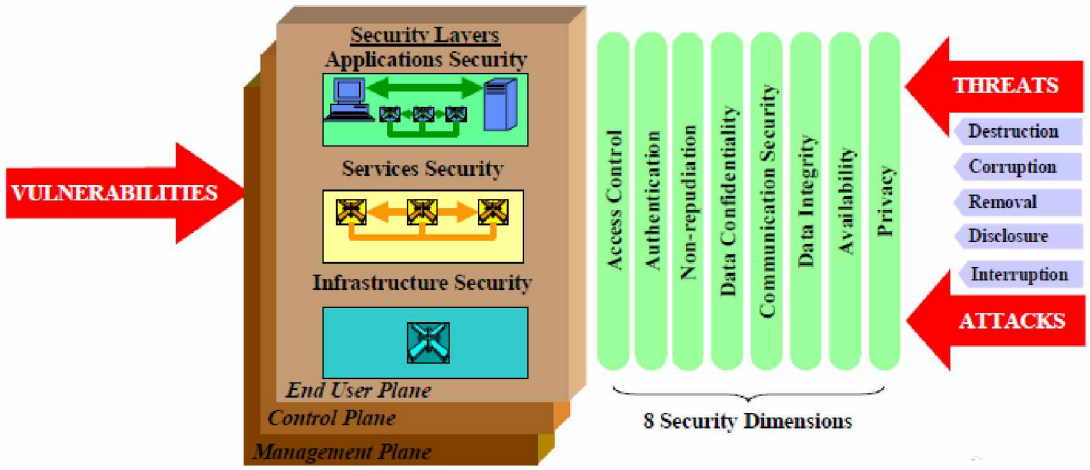

Рисунок 1 – Элементы архитектуры безопасности в ITU-T X.805

Одним из преимуществ определения уровней является возможность повторного использования в различных приложениях для обеспечения сквозной безопасности. Уязвимости на каждом уровне различны, поэтому необходимо определить меры противодействия для удовлетворения потребностей каждого уровня. Уровень инфраструктуры состоит из сетевых средств передачи, а также отдельных сетевых элементов. Примерами компонентов, принадлежащих уровню инфраструктуры, являются отдельные маршрутизаторы, коммутаторы и серверы, а также каналы связи между ними. Адреса уровня служб безопасность сетевых услуг, предлагаемых клиентам.

Эти услуги варьируются от базовых предложений подключения, таких как услуги выделенных линий, до дополнительных услуг, таких как обмен мгновенными сообщениями. Уровень приложений отвечает требованиям сетевых приложений, используемых клиентами. Эти приложения могут быть такими простыми, как электронная почта, или такими сложными, как совместная визуализация, когда высококачественная передача видео используется при разведке, например, нефти, проектировании сложной радиоэлектронной аппаратуры и т. д.

Вторая ось структуры касается безопасности действий, выполняемых в сети. Структура безопасности определяет три плоскости безопасности для представления трех типов защищенных действий, происходящих в сети. Плоскости безопасности: (1) плоскость управления, (2) плоскость управления и (3) плоскость конечного пользователя. Эти уровни безопасности удовлетворяют конкретные потребности безопасности, связанные с действиями по управлению сетью, действиями по управлению сетью или сигнализации и действиями конечного пользователя соответственно. Плоскость управления связана с действиями по эксплуатации, администрированию, обслуживанию и обеспечению (OAM&P), такими как предоставление пользователю или сети и т. д. Плоскость управления

связана с аспектами сигнализации для настройки (и изменения) сквозной связи через сеть независимо от среды и технологии, используемых в сети. Уровень конечного пользователя обеспечивает безопасность доступа и использования сети клиентами. Эта плоскость также занимается защитой потоков данных конечных пользователей.

Используя уровни безопасности и плоскости безопасности в качестве двух осей (3 плоскости безопасности и 3 уровня безопасности), структура также определяет восемь измерений, которые предназначены для обеспечения сетевой безопасности. С архитектурной точки зрения эти размеры применяются к каждой ячейке матрицы 3x3, образованной между слоями и плоскостями, чтобы можно было определить соответствующие меры противодействия. На рисунке 1 показаны плоскости, уровни и измерения безопасности архитектуры безопасности.

Конфиденциальность и конфиденциальность данных. Концепция конфиденциальности является фундаментальным мотиватором безопасности. Конфиденциальность обычно понимается как право отдельных лиц контролировать или влиять на то, какая информация, относящаяся к ним, может быть собрана и сохранена, а также кем и кому эта информация может быть раскрыта. В более широком смысле, конфиденциальность также связана с определенными техническими средствами (например, криптографией), гарантирующими, что эта информация не будет раскрыта никому, кроме предполагаемых сторон, так что только явно уполномоченные стороны могут интерпретировать контент, которым они обмениваются.

Чаще всего конфиденциальность и конфиденциальность данных используются как один и тот же термин, но следует отметить, что *ITU-T X.805* различает конфиденциальность и конфиденциальность данных, причем первая относится к защите ассоциации личности пользователей и действий, выполняемых их (например, привычки онлайн-покупок, посещаемые интернет-сайты и т.д.), причем последнее касается защиты от несанкционированного доступа к содержимому данных. Шифрование, списки контроля доступа и права доступа к файлам − это методы, которые часто используются для обеспечения конфиденциальности данных. Термин «конфиденциальность» упоминается в нескольких рекомендациях МСЭ-Т, включая F.115, H.235, J.160, Q.1531, X.800 и X.805.

Аутентификация. Аутентификация − это предоставление доказательства того, что заявленная личность объекта верна. Сущности здесь включают не только пользователей-людей, но также устройства, службы и приложения. Аутентификация также обеспечивает уверенность в том, что объект не пытается осуществить маскарад или несанкционированное воспроизведение предыдущего сообщения. Существует два типа аутентификации: аутентификация источника данных (т.е. аутентификация, запрошенная в ассоциации, ориентированной на соединение) и аутентификация однорангового объекта (т.е. аутентификация в ассоциации без установления соединения). Сеть должна гарантировать, что обмен данными установлен с адресованным одноранговым объектом (а не с объектом, пытающимся подделать или воспроизвести предыдущее установление) и что источник данных является заявленным. Аутентификация обычно следует за идентификацией. Информация, используемая для идентификации, аутентификации и авторизации, должна быть защищена сетью.

Целостность данных. Целостность данных – это свойство того, что данные не были изменены несанкционированным образом. В более широком смысле целостность данных также гарантирует, что информация защищена от несанкционированного изменения, удаления, создания и репликации, а также обеспечивает индикацию этих несанкционированных действий.

Важность телекоммуникационной безопасности:

− защита конфиденциальной информации. Телекоммуникационные сети переносят огромные объемы конфиденциальной информации, включая личные данные, финансовые операции и конфиденциальные деловые коммуникации. Обеспечение безопасности этих сетей является ключом к предотвращению несанкционированного доступа, утечки данных, кражи личных данных и финансового мошенничества;

– сохранение доступности сети. Телекоммуникационные сети должны быть всегда доступны и работоспособны для поддержки критически важных услуг, экстренной связи и бизнес-операций. Меры безопасности помогают предотвратить сбои, сбои в работе сети и атаки типа «отказ в обслуживании» (*DoS*), которые могут повлиять на подключение и услуги;

– защита национальной безопасности. Телекоммуникационные сети жизненно важны для национальной безопасности, поскольку они поддерживают связь между правительственными учреждениями, оборонными организациями и службами экстренной помощи. Безопасность этих сетей необходима для защиты от киберугроз, шпионажа и атак, нацеленных на критически важную инфраструктуру.

– поддержание доверия и репутации. Нарушения безопасности в телекоммуникационных сетях могут подорвать доверие к поставщикам услуг, что приведет к репутационному ущербу и оттоку клиентов. Уделяя приоритетное внимание безопасности телекоммуникаций, поставщики услуг могут продемонстрировать свою приверженность защите данных клиентов и поддержанию безопасной среды связи.

Проблемы в области телеком безопасности. Безопасность телекоммуникаций сталкивается с рядом проблем из-за постоянно меняющегося ландшафта угроз и сложности современных сетей связи. Некоторые из ключевых проблем включают в себя:

– сложные киберугрозы. Киберпреступники постоянно разрабатывают новые методы использования уязвимостей в телекоммуникационных сетях, таких как вредоносное ПО, программы-вымогатели, фишинговые атаки и сложные постоянные угрозы. Чтобы опережать эти угрозы, необходимы надежные меры безопасности и стратегии превентивной защиты.

– новые технологии. Внедрение новых технологий, таких как *5G*, Интернет вещей и облачные вычисления, создает новые риски и сложности в области безопасности. Защита этих технологий требует специальных знаний, обновленных протоколов безопасности и сотрудничества заинтересованных сторон;

– соответствие нормативным требованиям: поставщики телекоммуникационных услуг обязаны соблюдать различные правила и стандарты, касающиеся защиты данных, конфиденциальности и сетевой безопасности. Выполнение этих требований может оказаться сложной задачей, особенно для транснациональных организаций, работающих в разных юрисдикциях;

– инсайдерские угрозы. Инсайдерские угрозы, включая несанкционированный доступ сотрудников или подрядчиков, представляют значительный риск для безопасности телекоммуникаций. Внедрение средств контроля доступа, систем мониторинга и программ повышения осведомленности сотрудников имеет важное значение для смягчения этих угроз.

Уязвимости, угрозы и риски. При таком большом внимании к внедрению наиболее выгодных ИТ-решений или определению того, какие из новейших и лучших веб-приложений, серверов и баз данных лучше всего соответствуют целям организации, защита информации, хранящейся в этих активах, часто отводится на второй план. Многие предприятия могут быть обмануты, полагая, что, поскольку они не пострадали, значит, и угрозы нет.

Органы по стандартизации обладают уникальными возможностями и ответственностью устранять уязвимости безопасности в протоколах. Органы по стандартизации могут предпринять незамедлительные и относительно простые действия для повышения безопасности всех протоколов, которые в настоящее время стандартизируются.

Уязвимость безопасности – это недостаток или слабость в конструкции, реализации или работе системы, которая может быть использована для нарушения безопасности системы. Уязвимость безопасности не является риском, угрозой или атакой.

Уязвимости могут быть четырёх типов. Уязвимости модели угроз возникают из-за сложности предвидеть будущие угрозы (например, система сигнализации). Уязвимости

проектирования и спецификаций возникают из-за ошибок или упущений в разработке протокола, которые делают его уязвимым по своей сути (например, WEP в IEEE 802.11b, также известном как WiFi). Уязвимости реализации − это уязвимости, возникающие из-за ошибок в реализации протокола. Наконец, уязвимости эксплуатации и конфигурации возникают из-за неправильного использования опций в реализациях или слабых политик развертывания (например, необеспечения использования шифрования в сети Wi-Fi или выбора слабого потокового шифрования сетевым администратором).

Согласно X.800, угрозой безопасности является потенциальное нарушение безопасности, которое может быть активным (когда состояние системы может быть изменено) или пассивным (несанкционированное раскрытие информации без изменения состояния системы). Маскировка под авторизованный объект и отказ в обслуживании являются примерами активных угроз, а подслушивание с целью кражи четкого пароля — примером пассивной угрозы. Агентами угроз могут быть хакеры, террористы, вандалы, организованная преступность или спонсируемые государством, но в значительном количестве случаев угрозы исходят от инсайдеров организации.

Заключение. На основе анализа обеспечения безопасности телекоммуникационных систем можно предложить следующие мероприятия: внедрение строгого контроля доступа (используйте механизмы строгой аутентификации, такие как многофакторная аутентификация, чтобы гарантировать, что только авторизованные пользователи смогут получить доступ к сети и конфиденциальной информации); регулярное обновление (обновляйте все сетевые устройства, серверы и программное обеспечение с помощью новейших исправлений безопасности для устранения известных уязвимостей); шифрование сетевого трафика (используйте протоколы шифрования для защиты данных при передаче, предотвращая несанкционированный доступ и перехвата); регулярные проверки безопасности (проводите периодические проверки и оценки безопасности для выявления уязвимостей, оценки рисков и принятия необходимых мер безопасности).

Список литературы

1. *Security in Telecommunications and Information Technologyю An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications. Режим доступа: https://www.itu.int/ITU-T/edh/files/security-manual.pdf*

2. *Security for ICT - the work of ETSI. Режим доступа: https://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp1_security.pdf*

3. *Важность телекоммуникационной безопасности для обеспечения возможности подключения. Режим доступа: https://www.tuvsud.com/en-za/resource-centre/blogs/the-importance-of-telecom-security-safeguarding-connectivity*

UDC 621.3

SECURITY ASPECTS OF TELECOMMUNICATION SYSTEMS

Lutsky A.V.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Piskun G.A. – Cand. of Sci., assistant professor, associate professor of the department of ICSD

Annotation. Ensuring telecommunications security is shown to be critical to ensuring the integrity, confidentiality and availability of communication and data networks. Covers various aspects of protecting various components of the telecommunications infrastructure, including network devices, servers, databases, communication protocols and end-user devices.

Keywords: security, telecommunication systems, unauthorized access, security levels.