**УДК 004.056**

# ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СИСТЕМЕ ОРГАНИЗАЦИИ

**Щербов И.Л.,** декан факультета пожарной безопасности,
радиотехники и защиты информации,

**Якушина А.Е.,** ст. преподаватель
кафедры радиотехники и технической защиты информации,

**Тюрин Е.С.,** студент

Институт гражданской защиты Донбасса
ГВУЗ «Донецкий национальный технический университет»

*Проведен анализ программных и программно-аппаратных средств обеспечения информационной безопасности в ИТС организации. Рассмотрены технологии виртуальных сетей VLAN, практические аспекты применения средств защиты, в том числе систем предотвращения вторжений. С учетом рекомендаций международных стандартов ISO/IEC 27000; стандартов и лучших практик CobiT (Control Objectives for Information and related Technology); серии документов NIST 800 (National Institute of Standards and Technology); рекомендаций Международного союза электросвязи серии X «Сети передачи данных и взаимосвязь открытых сетей» (X800, X805) предложен перечень средств и технологий обеспечения безопасности ИТС, основанный на требованиях к уровню безопасности организации и бюджета, выделяемого на построение системы защиты.*

**Ключевые слова:** *информационно-телекоммуникационная система, средства обеспечения информационной безопасности, локальная вычислительная сеть.*

**Постановка проблемы и ее связь с актуальными научными и практическими исследованиями.**

В современном мире необходимость автоматизации, систематизации и ускорения производственных процессов является одним из ключевых факторов, повышающих эффективность труда. С этой целью информационные системы организаций объединяются в сеть, что обеспечивает необходимый доступ к общим ресурсам внутри организации, а так же к сети Интернет. При этом вопрос безопасности информационно-телекоммуникационных систем (ИТС) организации становится чрезвычайно актуальным.

С развитием информационных технологий растет количество угроз активам ИТС как извне, так и изнутри. Блокировка доступа к системе, несанкционированный доступ к конфиденциальным данным, выведение из строя того или иного компонента системы – это факторы, которые неблагоприятно сказываются на непрерывности бизнеса организации, ее престиже и доверии к ней.

Для решения задачи проектирования системы безопасности в информационно-телекоммуникационной системе организации предполагается наличие локальной вычислительной сети (LAN) организации, построенной на технологии Ethernet с возможным использованием компонентов WLAN (Wireless LAN). При проектировании архитектуры корпоративной сети необходимо учитывать такие свойства, как:

- простота внедрения;
- гибкость и масштабируемость;
- отказоустойчивость и безопасность;
- простота управления.

Основываясь на требованиях безопасности информационных систем и сетей, при проектировании LAN учитываются рекомендации таких нормативных документов, как: Серия международных стандартов ISO/IEC 27000; набор стандартов и лучших практик CobiT (Control Objectives for Information and related Technology); серия документов NIST 800 (National Institute of Standards and Technology); рекомендации Международного союза электросвязи серии X «Сети передачи данных и взаимосвязь открытых сетей» (X800, X805) и других нормативно-правовых документов. Однако на практике почти всегда возникают разногласия между сотрудниками ИТ-подразделений и бизнес-подразделений на фоне неприемлемого процесса взаимного функционирования внедренных систем (бизнес-задач и систем безопасности). Также всегда учитывается стоимость приобретаемых средств защиты. Поэтому вопрос проектирования системы безопасности является более глубоким и требует рассмотрения большого ряда аспектов.

**Изложение основного материала исследования.** Обеспечение безопасности сетевой архитектуры организации требует комплексного подхода, который включает в себя разработку нормативной документации, решение вопросов управления рисками, построение физической безопасности, решение вопросов непрерывности бизнеса и восстановления после аварий, собственно построение системы сетевой безопасности, и все это должно быть выстроено с учетом требований законодательных нормативов и рекомендаций международных практик.

Соответственно, возникает вопрос в выборе средств защиты. Это могут быть программные, аппаратные или программно-аппаратные средства. В зависимости от уровня конфиденциальности обрабатываемой информации определяются допустимые риски от возможной реализации угроз безопасности информации и, соответственно, бюджет, выделяемый на внедрение средств защиты.

Рассмотрим пример архитектуры ИТС (рис. 1).

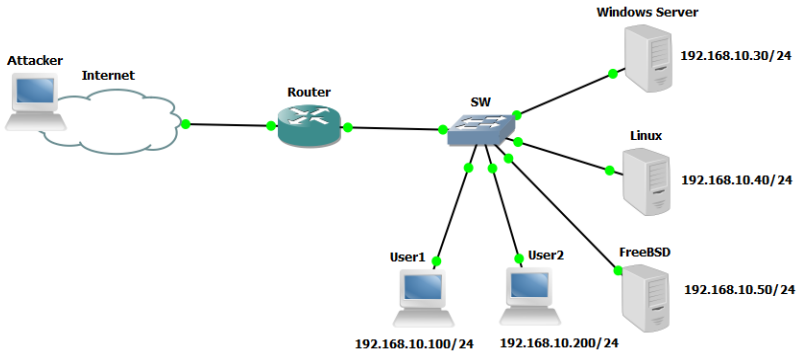


Рис.1. Схема сети ИТС

Данная схема не является эталонной, может быть изменена в зависимости от требований организации, количество любых устройств (сетевых, периферии, локальных компьютеров, серверного оборудования) может быть изменено.Для данной схемы ИТС сложно указать, какие именно места являются уязвимыми, т.к. все определяется конфигурацией устройств и установленным программным обеспечением.

Например, постоянное обновление компонентов систем до актуальных версий является минимально-необходимым требованием, поскольку с новыми обновлениями закрываются бреши безопасности приложений, обновляются сигнатуры угроз. Но при неправильном конфигурировании сетевых устройств данные обновления становятся бесполезными. Поэтому возникает необходимость использования комплексного подхода, при котором будет учтено максимальное количество аспектов сетевой безопасности.

Использование технологии виртуальных сетей VLAN (Virtual LAN) позволяет разделить и сгруппировать компьютеры логически, основываясь на необходимых им ресурсах, безопасности и потребностях бизнеса.

На рис.1 пользователю User1 нужно иметь доступ только к WindowsServer и Linux, а пользователю User2 – только к FreeBSD. Технология VLAN позволит настроить на коммутаторе SW маршруты, согласно которым все потоки данных будут проходить только по заранее определенным маршрутам между пользователями в пределах своего VLAN. Это позволяет исключить нежелательное ознакомление пользователей с непредназначенной для них информацией. Кроме того, находясь в пределах одного VLAN, потенциальному злоумышленнику будет гораздо сложнее получить доступ к ресурсам из другой виртуальной сети.

Технология NAT (Network Address Translation – Трансляция сетевых адресов) не только помогает временно решить проблему уменьшения числа свободных IP-адресов, но также позволяет скрыть внутренние адреса сети, объединяя их на одном устройстве.

Любые исходящие из сети кадры имеют в качестве адреса источника только адрес этого устройства, а не фактический адрес компьютера, отправившего данные. Это позволяет, например, существенно ослабить вероятность успешного сканирования внутренней сети организации, что является первым шагом перед направленной атакой.

В случае, когда было принято решение пользоваться беспроводными технологиями WLAN (Wireless LAN), крайне важно конфигурировать оборудование с учетом стандартов 802.11i.

Более старые версии не обеспечивают должной защиты.

Ключ, зашифрованный с использованием протокола WEP (Wired Equivalent Privacy), может быть взломан с использованием открытого программного обеспечения, например, «AirCrack», затратив при этом 5-10 минут (рис. 2).

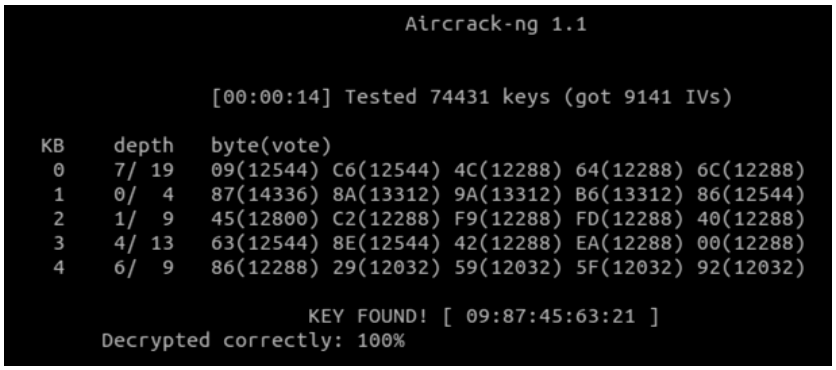


Рис. 2. Быстрый взлом ключа шифрования WEP

Использование стандартов 802.11i и более поздних версий обеспечивает более высокую надежность, благодаря внедренным надежным алгоритмам шифрования TKIP, AES, CCMP. Взлом ключа в таком случае будет зависеть от сложности установленного администратором пароля. Также стоит учитывать, что даже при включении шифрования WPA/WPA2 на беспроводном маршрутизаторе, во многих устройствах заводскими настройками включена технология WPS (Wi-Fi Protected Setup) со старой уязвимостью, позволяющей получить доступ к точке доступа за вполне приемлемое время – от нескольких часов до нескольких суток, например с использованием свободного ПО «reaver» (рис. 3).

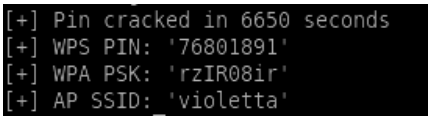


Рис. 3. Взлом ключа WPA2 с использованием уязвимости стандарта WPS

Также следует учитывать, что аутентификация пользователя обеспечивает более высокую степень уверенности и защиты, чем аутентификация системы. Поэтому для аутентификации системы рекомендуется устанавливать сервер аутентификации, например RADIUS. Он дает возможность предотвратить передачу трафика до тех пор, пока пользователь не будет должным образом авторизован.

Перечисленные выше методы обеспечения безопасности ИТС преимущественно реализуются программными методами, с использованием бесплатного open-source ПО, т.е. они не требуют слишком больших дополнительных денежных затрат. Безусловно, часть технологий реализуется непосредственно на маршрутизаторах или коммутаторах, которые имеют разную стоимость. Однако они в любом случае будут присутствовать в счете ИТС и их приобретение является необходимостью.

Все же, когда требования к безопасности сети более высоки, невозможно не выделить программные и программно-аппаратные средства, такие как межсетевые экраны и системы обнаружения и предотвращения вторжений IPS/IDS. Для указанной выше схемы сети (рис. 1) с целью разграничения доступа система IPS уровня сети (NIPS) устанавливается в разрез между маршрутизатором Router, ведущим во внешнюю сеть, и коммутатором (SW), как показано на рис. 4.

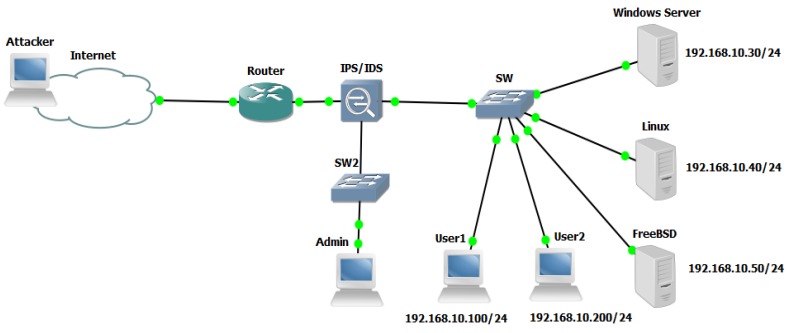


Рис. 4. Включение NIPS в разрез сети

Такое включение обеспечивает трансляцию всего трафика через устройство. Первичную фильтрацию может обеспечить маршрутизатор, однако он не позволяет выявлять и предотвращать сетевые атаки.

Для демонстрации эффективности работы IPS, построим схему в среде моделирования GNS3, изображенную на рис. 4.

Предполагаемый атакующий Attacker располагается во внешней сети. Следует иметь в виду, что в 80 % организаций IPS не настраиваются должным образом. Это обусловлено тем, что их просто некому настроить или система установлена только «для галочки», чтобы соответствовать тем или иным требованиям регуляторов.

Примером тому может служить простое сканирование хостов сети с использованием утилиты «nmap». При проведении простого SYN-сканирования хостов подсети 192.168.10.x/24 была выявлена операционная система Windows XP (SP3) на хосте 192.168.10.200 и Windows Server 2003 на хосте 192.168.10.30.

Данные версии операционной системы имеют давно известную уязвимость MS08-067, и если не были установлены обновления и применены патчи, то появляется реальная угроза выполнения произвольного кода на целевой системе с привилегиями учетной записи SYSTEM (Windows XP) и отказа в обслуживании (Windows Server 2003). Используя фреймворк Metasploit Framework, уязвимость была проэксплуатирована на хосте Windows XP, в результате чего появился доступ к командной строке хоста-жертвы:

*[*] Started bind handler*
*[*] Automatically detecting the target…*
*[*] Fingerprint: Windows XP Service Pack 3 – lang:Russian*
*[*] Selected Target: Windows XP SP3 Russian (NX)*
*[*] Triggering the vulnerability…*
*[*] Command shell session 1 opened (192.168.20.1:5583 -> 192.168.10.200:7777)*

Microsoft Windows XP [‚¥àá¨ï 5.1.2600]
(‘) Š®à¯®à æ¨ï Œ ©ªà®á®äâ, 1985-2001.
C:\WINDOWS\system32>

Соответственно, теперь имеется доступ к системе жертвы. При повышении привилегий до уровня Администратора появляется полный контроль над системой. Ущерб в данном случае будет определяться всеми возможными факторами: стоимость утраченной информации, ущерб от возможного отказа работы всех установленных служб и программ, возможный доступ к другим устройствам и компонентам сети и т.д.

Если же правильно и тщательно настроить IPS, то само сканирование уже не будет выполнено успешно. Современные устройства NIPS позволяют гибко настроить правила фильтрации и анализа. К примеру, установив блокирование всех хостов, с которых идет трафик, содержащий информацию о попытках SYN-сканирования, дальнейшие действия злоумышленника не будут успешны для его сетевого адреса. После установления такого правила, утилита “nmap” выполняла так называемое «тихое», «безопасное» SYN-сканирование очень долго и не вывела никаких результатов. Таким образом, грамотная настройка сетевых устройств позволяет существенно сократить риск успешных атак на целевую систему и сеть в целом.

**Выводы и перспективы дальнейших исследований.** В данной работе рассмотрены основные методы и способы защиты информации ИТС организации, позволяющие снизить себестоимость предоставляемых услуг; обоснована необходимость квалифицированного подхода при конфигурировании применяемых систем защиты информационной.

**Библиографический список**

1. Воропаева В.Я., Щербов И.Л. Адаптация информационно-телекоммуникационных систем к внешним воздействиям» // Научные труды Донецкого национального технического университета. Серия: «Вычислительная техника и автоматизация». – Выпуск 23 (201). – Донецк, ДонНТУ, 2012. – С. 83-88.

2. Информационные технологии. Методы и средства достижения информационной безопасности. Системы управления информационной безопасностью. Требования (ISO/IEC 27001:2005, IDT): ДСТУ ISO/IEC 27001:2010. – [Введения 2012-07-01]. – К.: Издательство Украины 2012. – (Национальный стандарт Украины).

3. CISSP All-in-One Exam Guide, 5th Ed. / Harris / 160217-8.

4. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: Учебник для вузов. 4-е изд. – СПб.: Питер, 2010. – 944 с.: с ил.

5. Воропаева В.Я., Щербов И.Л., Хаустова Е.Д. Управление информационной безопасностью информационно-телекоммуникационных систем на основе модели «PLAN-DO-CHECK-ACT»» // Научные труды ДонНТУ. Серия: «Вычислительная техника и автоматизация». – Выпуск 2 (25). – Донецк, ДонНТУ, 2013.

6. NIST Special Publication 800-115. Technical Guide to Information Security Testing and Assessment.


*E-mail: scherbov@yandex.ua*
*Рецензент к.т.н., доц. В.В. Паслён*