Пономарев Артем Николаевич
старший преподаватель
МИРЭА - Российский Технологический Университет
г. Москва

УПРАВЛЕНИЕ БЕЗОПАСНОСТЬЮ БЕСПРОВОДНОЙ ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ

Аннотация. Предложена методика, цель которой реализация эффективного процесса управления безопасностью в беспроводных локальных вычислительных сетях. Для достижения результата используются математические вычисления качественных характеристик различного рода критериев, определяющих необходимый уровень защищенности сети.

Ключевые слова: информационная безопасность, беспроводная сеть, локальная сеть, управление безопасностью, уровень защищенности, маршрутизатор, точка доступа, уязвимость, риск.

Требование мобильности пользователя информационной инфраструктуры привело к повсеместному применению беспроводных локальных вычислительных сетей (БЛВС). Вместе с тем уязвимости технологий беспроводной связи приводят к появлению большого количества атак при передаче информации, также увеличивается и вероятность несанкционированного доступа, что может вызвать дополнительную загрузку канала передачи данных, утрату паролей и другой конфиденциальной информации пользователя. Ввиду этого актуальной становится проблема защиты локальной беспроводной сети от внешних угроз, и, в частности, точка доступа, которая является наиболее уязвимым местом в ней [1].

Целью исследования является разработка методики управления безопасностью БЛВС, с учетом угроз, исходящих из внешнего по отношению к сети периметра. Большинство технологий беспроводного абонентского доступа строится на основе компьютерной сети [2].

Для достижения указанной цели необходимо решить следующие задачи:

– установить требуемый уровень защищенности БЛВС;

– оценить ее текущую защищенность;

– определить меры, позволяющие обеспечить требуемый уровень защищенности.

Данный алгоритм действий позволит наиболее целостно и обоснованно выстроить защиту локальной сети, избежать возможных рисков, а также выдержать баланс между затрачиваемыми ресурсами и получаемым результатом (рис. 1), что является одним из основных критериев выбора систем безопасности [3].

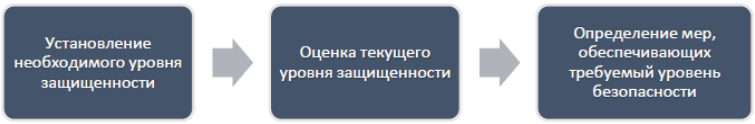

Рис. 1. Процесс управления безопасностью в локальной сети

Любую архитектуру системы обеспечения безопасности сети и состав ее компонентов необходимо строить с учетом актуальных угроз, ценности защищаемых активов (как количественных, так и качественных) и вероятности реализации угроз. Исходя из этого, при управлении безопасностью БЛВС нужно оперировать требованиями, на основе которых будет выстраиваться защита сети [4].

На первом этапе устанавливается необходимый уровень защищенности (НУЗ). Он определяется принадлежностью сети, количеством пользователей, характером передаваемой информации, а также ценностью подключаемых устройств (Табл. 1).

Определение необходимого уровня защищенности даст целостное представление о функционирующей сети и ее ценности с точки зрения важности информации и сетевых ресурсов, а также обусловит выбор способов достижения информационной безопасности. необходимый уровень защищенности можно определить:

$$НУЗ = (T + C + M + V) \cdot 0{,}1 \quad (1)$$

где T — оценка критерия «тип сети»; C — оценка критерия «число пользователей»; M — оценка критерия «характер информации»; V — оценка критерия «ценность технических средств в сети».

Таблица 1 - Критерии для оценки необходимого уровня защищенности сети

№	Критерий	Значение	Оценка
1	Тип сети (T)	общедоступная	5
		домашняя	15
		корпоративная	25
2	Число пользователей (C)	до 10 чел.	5
		до 100 чел	15
		свыше 100 чел.	25
3	Характер информации (M)	общедоступная	5
		частная (персональные данные)	15
		служебная (конфиденциальная)	25
4	Ценность устройств в сети (V)	до 100 тыс. рублей	5
		до 1 млн рублей	15
		свыше 1 млн рублей	25

Результатом данного этапа является определение необходимого уровня защищенности сети, согласно полученной оценке, показанной в таблице ниже (табл. 2).

Таблица 2 - Определение необходимого уровня защищенности

Уровень защищенности	Оценка НУЗ
1 уровень (начальный)	до 0,2
2 уровень	0,2 … 0,4
3 уровень (средний)	0,4 … 0,6
4 уровень	0,6 … 0,8
5 уровень (высокий)	0,8 и выше

На втором этапе определяется текущий уровень защищенности (ТУЗ) локальной сети, который основывается на энергетических характеристиках и конфигурациях маршрутизатора (Wi-Fi-роутера):

$$ТУЗ = SL \cdot PL \cdot 0{,}1, \quad (2)$$

где PL (power layer) — оценка защищенности на энергетическом уровне; SL (switch layer) — оценка защищенности на уровне маршрутизатора.

Расчет оценки производится путем суммирования оценок по каждому критерию так, что: низкий уровень равен 1, средний — 2 и высокий — 3.

$$PL = P + F + Pr\ , \quad (3)$$

где PL (power layer) — оценка энергетической доступности; P (position) — значение защищенности, соответствующее месту расположения; F (frequency) — значение защищенности, соответствующее частоте функционирования маршрутизатора; Pr (power) — значение защищенности, соответствующее мощности исходящего сигнала.

Уровень безопасности может быть низким, средним или высоким (Табл. 3).

Таблица 3 - Критерии оценки уровня защищенности маршрутизатора

Характеристика	Уровень безопасности		
	Низкий	Средний	Высокий
Пароль	состоит из цифр и букв в нижнем регистре разрядность до 8 символов	состоит из цифр и букв в нижнем и верхнем регистре разрядность до 10 символов	состоит из цифр и букв в нижнем и верхнем регистре, специальных символов разрядность свыше 10 символов
Метод шифрования	WEP	WPA/WPA2	WPA3
WPS	включен	-	Отключен
Количество устройств	не ограничено	ограничено с большим запасом	ограничено с незначительным запасом
Фильтрация по MAC	не настроена	-	Настроена
SSID	отражает производителя и/или модель оборудования	идентифицирует данные о пользователе оборудования	неприметный, не отражает действительной информации

Учетная запись администратора оборудования	заводские учетные данные	учетные данные, настроенные представителем провайдера	учетные данные собственно созданные
UPnP-статус	включен	-	отключен
Брандмауэр	отключен	-	включен
VPN	отключен	-	включен

Расчет оценки производится путем суммирования оценок по каждому критерию так, что низкий уровень – это 0, средний – 5 и высокий – 10. Суммарный показатель – оценка защищенности на уровне маршрутизатора — можно определить:

$$SL = \sum_{i=1}^{10} N(i), \quad (4)$$

где SL (switch layer) — оценка защищенности на уровне маршрутизатора; N(i) (power layer) — оценка i-го критерия.

Данное значение позволяет соотнести локальную сеть к тому или иному уровню защищенности и выбрать соответствующие меры защиты (Табл. 4).

Таблица 4 - Определение текущего уровня защищенности

Уровень защищенности	Оценка ТУЗ
1 уровень (начальный)	до 20
2 уровень	20 … 40
3 уровень (средний)	40 … 60
4 уровень	60 … 80
5 уровень (высокий)	80 и выше

На последнем этапе, в случае несоответствия текущего уровня защищенности требуемому, определяются меры, которые должны быть приняты для достижения необходимого уровня защищенности. Для этого идет корректировка существующих и, в случае необходимости, введение дополнительных элементов защиты локальной сети (Табл. 5).

Таблица 5 - Требования к безопасности сети

Уровень защищенности	Требования к безопасности сети
1 уровень	использование паролей низкой сложности, применение шифрования WPA/WPA2, без ограничения энергетической доступности
2 уровень	использование паролей средней сложности, применение шифрования WPA/WPA2, отключенный WPS, учетная запись администратора собственно создана, без ограничения энергетической доступности
3 уровень	использование паролей средней сложности, применение шифрования WPA/WPA2, учетная запись администратора собственно создана, SSID не отражает действительной информации, учитывается расположение роутера
4 уровень	использование паролей высокой сложности, применение шифрования WPA/WPA2, SSID не отражает действительной информации, учетная запись администратора создана, осуществляется фильтрация по MAC, UPnP- статус отключен, ограничивается количество пользователей, учитывается расположение роутера и частоты функционирования
5 уровень	использование паролей высокой сложности, применение шифрования WPA3, SSID не отражает действительной информации, учетная запись администратора собственно создана, осуществляется фильтрация по MAC, UPnP-статус отключен, ограничивается количество пользователей, используются дополнительные сервисы (Брандмауэр, VPN), учитываются все критерии энергетической доступности

Выводы. Развитие технологий построения локальных сетей стимулирует совершенствование способов проведения кибератак злоумышленниками. Вместе с тем существующие угрозы в киберпространстве способствуют совершенствованию новых практик по снижению рисков информационной безопасности. Для этого в рамках данной работы была разработана методика управления безопасностью беспроводной локальной вычислительной сети, которая позволяет установить необходимый уровень защищенности и, на основе вычислений, определить соответствие текущего уровня защищенности сети требуемому, а также реализовать меры, позволяющие привести безопасность сети в соответствие с требуемым уровнем.

Список литературы:

1. Соколов А. В., Шаньгин В. Ф. 2016. Защита информации в распределенных корпоративных сетях и системах. М., ДМК Пресс, 656.

2. Баринов В. В., Баринов И. В., Пролетарский А.В. 2018. Компьютерные сети: Учебник. М., Academia, 192.

3. Малюк, А.А. 2016. Информационная безопасность: концептуальные и методологические основы защиты информации. М., ГЛТ, 280.

4. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. 2014. Защита информации в сети — анализ технологий и синтез решений. М., ДМК Пресс, 615.