УДК 004.056.2
DOI 10.52575/2687-0932-2023-50-1-183-190

Управление безопасностью беспроводной локальной вычислительной сети

Адгемов И.Э., Девицына С.Н.
Севастопольский государственный университет,
Россия, 299053, г. Севастополь, ул. Университетская, д. 33
E-mail: ilmmov_95@mail.ru, sndevitsyna@sevsu.ru

Аннотация. Предложена методика, целью которой является реализация эффективного процесса управления безопасностью в беспроводных локальных вычислительных сетях. Для достижения результата используются математические вычисления качественных характеристик различного рода критериев, определяющих необходимый и текущий уровень защищенности сети. Анализ безопасности сети проводится в рамках угроз, исходящих из внешнего периметра. В ходе анализа и вычислений устанавливаются обоснованные требования к уровню безопасности беспроводных локальных сетей, производится текущая оценка защищенности сети и, в результате, определяются меры, позволяющие достичь необходимый уровень безопасности сети. Данная методика может быть использована для частных целей, а также как часть комплексного обеспечения безопасности в государственных и коммерческих организациях.

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

Для цитирования: Адгемов И.Э., Девицына С.Н. 2023. Управление безопасностью беспроводной локальной вычислительной сети. Экономика. Информатика, 50(1): 183–190. DOI 10.52575/2687-0932-2023-50-1-183-190

Wireless Network Security Management

Ilmir E. Adgemov, Svetlana N. Devitsyna
Sevastopol State University,
33 University St, Sevastopol, 299053, Russia
E-mail: ilmmov_95@mail.ru, sndevitsyna@sevsu.ru

Abstract. This paper presents a technique that aims to implement an effective security management process in wireless networks. To achieve the goal, the technique uses mathematical calculations of the qualitative characteristics of various criteria that determine the required level of security and the current level of network security. Network security analysis is carried out for threats emanating from the external perimeter, intruders using special hardware and software to attack the border router and network users. The result of the analysis and calculations are reasonable requirements for the level of security of wireless networks, a current assessment of the security of the network is made and, as a result, measures are determined to achieve the required level of network security. This technique can be used for private purposes, as well as part of a comprehensive security in government and commercial organizations.

Keywords: information security, wireless network, local area network, security management, security level, router, access point, vulnerability, risk

For citation: Adgemov I.E., Devitsyna S.N. 2023. Wireless Network Security Management. Economics. Information technologies, 50(1): 183–190 (in Russian). DOI 10.52575/2687-0932-2023-50-1-183-190

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 [Соколов, Шаньгин, 2016; Чипига, 2017; Шелухин, 2013]. На схеме (рис. 1) показаны варианты реализации кибератак на БЛВС.

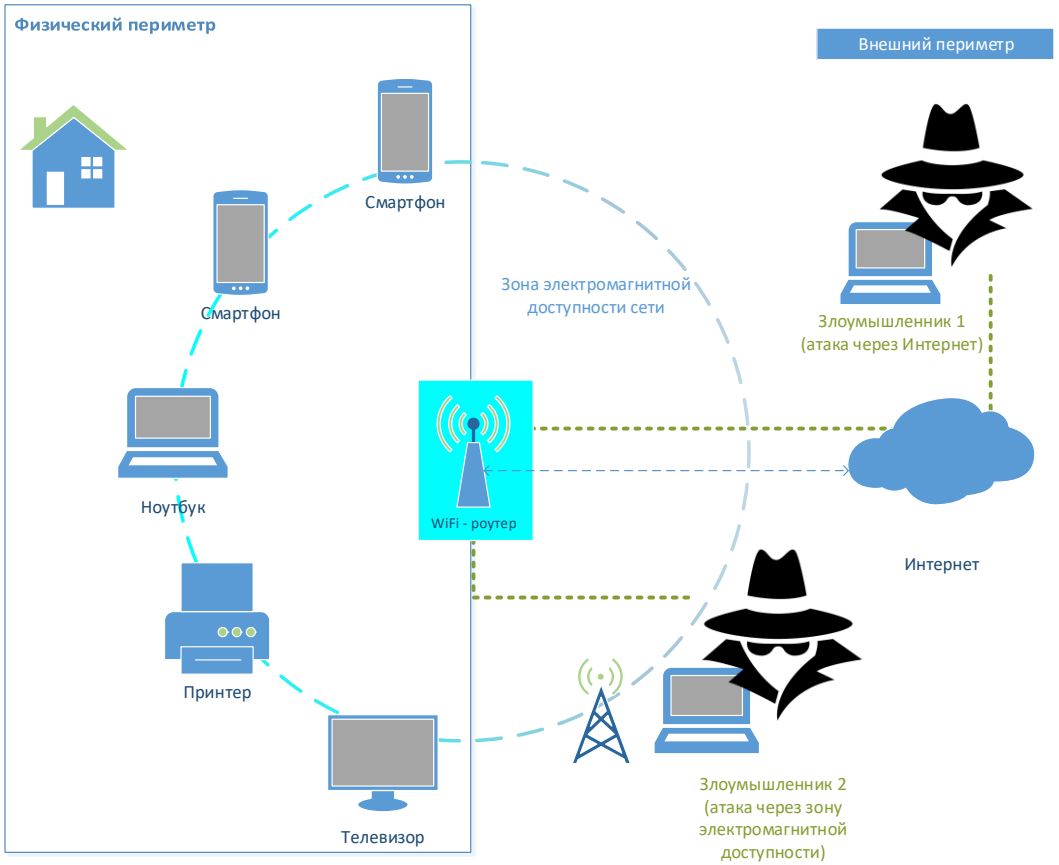

Рис. 1. Схема реализации атак на беспроводную ЛВС
Fig. 1. Implementation of attacks on a wireless network

Целью исследования является разработка методики управления безопасностью БЛВС (information security management), с учетом угроз, исходящих из внешнего по отношению к сети периметра. Большинство технологий беспроводного абонентского доступа строится на основе компьютерной сети [Астахова, 2013; Баринов и др., 2018; Громов, 2017; Кузин, 2013; Кузьменко, 2013; Максимов, 2017; Новиков, 2011; Прончев, 2009; Расстригин, 2015].

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. 2), что является одним из основных критериев выбора систем безопасности [Малюк, 2016; Новиков и др., 2017; Олифер и др., 2016].

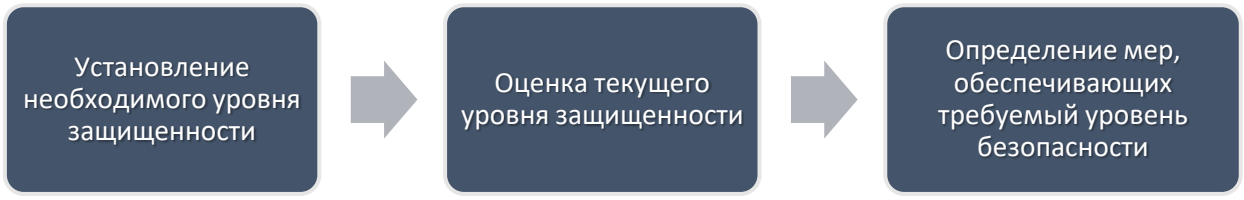

Рис. 2. Процесс управления безопасностью в локальной сети
Fig. 2. The process of managing security in a local network

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 [Галицкий и др., 2014; Лаборатория знаний, 2013; Новожилов, 2018; Попов, 2004; Шубин, Красильников, 2013].

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:

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

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
Table 1

Критерии для оценки необходимого уровня защищенности сети
Criteria for assessing the required level of network security

№	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

Окончание табл. 1
End table 1

№	Критерий	Значение	Оценка
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
Table 2

Определение необходимого уровня защищенности
Determination of the required level of security

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):

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

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

Критерии оценки энергетической доступности показаны в таблице (Табл. 3).

Таблица 3
Table 3

Критерии оценки энергетической доступности
Criteria for assessing energy availability

Характеристика	Уровень безопасности		
	Низкий	Средний	Высокий
Расположение маршрутизатора	На границе необходимого для покрытия периметра	В позиции, смещенной от центра периметра	В середине необходимого для покрытия периметра
Частота функционирования	2,5 ГГц	2,5 ГГц и 5 ГГц	5 ГГц
Мощность сигнала	Высокая	Средняя	Низкая

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

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

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

Уровень безопасности может быть низким, средним или высоким (Табл. 4).

Таблица 4
Table 4

Критерии оценки уровня защищенности маршрутизатора
Criteria for evaluating the router's security level

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. 5).

Таблица 5
Table 5

Определение текущего уровня защищенности
Determination of the current security level

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. 6).

Таблица 6
Table 6

Требования к безопасности сети
Network security requirements

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

Астахова И.Ф. 2013. Компьютерные науки. Деревья, операционные системы, сети. М., Физматлит, 88.
Баринов В.В., Баринов И.В., Пролетарский А.В. 2018. Компьютерные сети: Учебник. М., Academia, 192.
Беспроводные сети Wi-Fi. М., Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2013.
Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. 2014. Защита информации в сети — анализ технологий и синтез решений. М., ДМК Пресс, 615.
Громов Ю.Ю. 2017. Информационная безопасность и защита информации: Учебное пособие. Ст. Оскол, ТНТ, 384.
Кузин А.В. 2013. Компьютерные сети: Учебное пособие. М., Форум, НИЦ Инфра-М, 192.
Кузьменко Н.Г. 2013. Компьютерные сети и сетевые технологии СПб., Наука и техника, 368.
Максимов Н.В. 2017. Компьютерные сети: Учебное пособие. М., Форум, 320.
Малюк, А.А. 2016. Информационная безопасность: концептуальные и методологические основы защиты информации. М., ГЛТ, 280.
Новиков Ю.В. 2011. Аппаратура локальных сетей: функции, выбор, разработка. М., Эком, 288.
Новиков Ю.В., Карпенко Д.Г. 2017. Аппаратура локальных сетей: функции, выбор, разработка. М., Эком, 288.
Новожилов Е.О. 2018. Компьютерные сети: Учебное пособие. М., Академия, 176.
Олифер В.Г., Олифер Н.А. 2016. Компьютерные сети. Принципы, технологии, протоколы: Учебник. СПб., Питер, 176.
Попов И.И., Максимов Н.В. 2004. Компьютерные сети. М., Форум, 336.
Прончев Г.Б. 2009. Компьютерные коммуникации. Простейшие вычислительные сети: Учебное пособие. М., КДУ, 64.
Расстригин Л.А. 2015. Вычислительные машины, системы, сети. М., Наука, 224.
Соколов А.В., Шаньгин В.Ф. 2016. Защита информации в распределенных корпоративных сетях и системах. М., ДМК Пресс, 656.
Чипига А.Ф. 2017. Информационная безопасность автоматизированных систем. М., Гелиос АРВ, 336.
Шелухин О.И. 2013. Обнаружение вторжений в компьютерные сети (сетевые аномалии). М., ГЛТ, 220.
Шубин В.И., Красильникова О.С. 2013. Беспроводные сети передачи данных. М., Вузовская книга, 104.

References

Astakhova I.F. 2013. Computer science. Trees, operating systems, networks. M., Fizmatlit, 88. (in Russian)
Barinov V.V., Barinov I.V., Proletarsky A.V. 2018. Computer networks: Textbook. M., Academia, 192. (in Russian)
Wireless Wi-Fi networks. M., Internet University of Information Technologies, Binom. Knowledge Lab, 2013. (in Russian)
Galitsky A.V., Ryabko S.D., Shangin V.F. 2014. Protection of information in the network — analysis of technologies and synthesis of solutions. M., DMK Press, 615. (in Russian)
Gromov Y.Y. 2017. Information Security and Information Protection: Textbook. Art. Oskol, TNT, 384. (in Russian)
Kuzin A.V. 2013. Computer networks: Textbook. M., Forum, NIC Infra-M, 192. (in Russian)
Kuzmenko N.G. 2013. Computer networks and network technologies, St. Petersburg, Science and technology, 368. (in Russian)

Maksimov N.V. 2017. Computer networks: Textbook. M., Forum, 320. (in Russian)
Malyuk, A.A. 2016. Information security: conceptual and methodological foundations of information security. M., GLT, 280. (in Russian)
Novikov Y.V. 2011. Local area network equipment: functions, selection, development. M., Ekom, 288 (in Russian)
Novikov Y.V, Karpenko D.G. 2017. Local area network equipment: functions, selection, development. M., Ekom, 288. (in Russian)
Novozhilov E.O. 2018. Computer networks: Textbook. M., Academy, 176. (in Russian)
Olifer V.G., Olifer N.A. 2016. Computer networks. Principles, technologies, protocols: Textbook. SPb., Peter, 176. (in Russian)
Popov I.I., Maksimov N.V. 2004. Computer networks. M., Forum, 336. (in Russian)
Pronchev G.B. 2009. Computer communications. The simplest computer networks: Textbook. M., KDU, 64. (in Russian)
Rasstrigin L.A. 2015. Computers, systems, networks. M., Nauka, 224. (in Russian)
Sokolov A.V., Shangin V.F. 2016. Information protection in distributed corporate networks and systems. M., DMK Press, 656. (in Russian)
Chipiga A.F. 2017. Information security of automated systems. M., Helios ARV, 336. (in Russian)
Shelukhin O.I. 2013. Computer network intrusion detection (network anomalies). M., GLT, 220. (in Russian)
Shubin V.I., Krasilnikova O.S. 2013. Wireless data transmission networks. M., Vuzovskaya book, 104. (in Russian)

Конфликт интересов: о потенциальном конфликте интересов не сообщалось.
Conflict of interest: no potential conflict of interest related to this article was reported.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Адгемов Ильмир Эльдарович, магистрант кафедры «Информационная безопасность» института информационных технологий Севастопольского Государственного университета, г. Севастополь, Россия

Девицына Светлана Николаевна, кандидат технических наук, доцент, доцент кафедры «Информационная безопасность» института информационных технологий Севастопольского Государственного университета, г. Севастополь, Россия

INFORMATION ABOUT THE AUTHORS

Ilmir E. Adgemov, Master student of the Department "Information Security", Institute of Information Technologies, Sevastopol State University, Sevastopol, Russia

Svetlana N. Devitsyna, Candidate of Technical Sciences, Associate Professor, Associate Professor of the Department "Information Security", Institute of Information Technologies, Sevastopol State University, Sevastopol, Russia