Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт **информационных технологий и телекоммуникаций**
Кафедра **организации и технологии защиты информации**

Утверждена распоряжением по институту
от «12» марта 2020 г. № 028-р/12.00
Выполнена по заявке организации
(предприятия) ООО «Медиа-техника»
г. Ставрополь

Допущена к защите
« 20 » июня 2020 г.
Зав. кафедрой организации и технологии защиты информации
канд. техн. наук, доцент
В.И. Петренко

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА
АНАЛИЗ ЗАЩИЩЕННОСТИ ПЕРСПЕКТИВНОЙ СЕТИ IEEE 802.11AX С ОБОСНОВАНИЕМ МЕР ПО ЕЕ ЗАЩИТЕ

Рецензенты:
Самойленко Ирина Владимировна
канд. техн. наук, доцент, доцент кафедры информационных систем ФГБОУ ВО «Ставропольский государственный аграрный университет»

Нормоконтролер:
Рачков Валерий Евгеньевич
канд. техн. наук, доцент, доцент кафедры организации и технологии защиты информации

(*подпись*)

Дата защиты «02» июля 2020 г.

Оценка _____

Выполнил:
Заводнов Вячеслав Сергеевич
студент 2 курса, ИНБ-м-о-18-1 группы направления подготовки 10.04.01 «Информационная безопасность» направленность (профиль) «Комплексная защита объектов информатизации» очной формы обучения

(*подпись*)

Руководитель:
Рачков Валерий Евгеньевич
канд. техн. наук, доцент, доцент кафедры организации и технологии защиты информации

(*подпись*)

Ставрополь, 2020 г.

СОДЕРЖАНИЕ

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт	**информационных технологий и телекоммуникаций**
Кафедра	**организации и технологии защиты информации**
Направление подготовки	**Информационная безопасность**
Направленность (профиль)	**Комплексная защита объектов информатизации**

УТВЕРЖДАЮ
Зав. кафедрой организации и технологии защиты информации
канд. техн. наук, доцент
В.И. Петренко
«04» апреля 2020 г.

ЗАДАНИЕ НА ВЫПУСКНУЮ КВАЛИФИКАЦИОННУЮ РАБОТУ (ДИПЛОМНУЮ РАБОТУ)

Студент Заводнов Вячеслав Сергеевич группа ИНБ-м-о-18-1

1. Тема Анализ защищенности перспективной сети IEEE 802.11ax с обоснованием мер по ее защите

Утверждена распоряжением по институту «12» марта 2020 г. № 028-р/12.00

2. Срок представления работы к защите «29» июня 2020 г.

3. Исходные данные для исследования Выпускную квалификационную работу выполнить в соответствии с положениями: ГОСТ Р 57628-2017 Информационная технология (ИТ). Методы и средства обеспечения безопасности; ГОСТ Р 57640-2017 Информационные технологии. Эталонная модель процесса (ЭМП) для управления ИБ.

4. Содержание ВКР:

4.1 Анализ системы управления компании и актуализация угроз информации.

4.2 Анализ защищенности перспективной сети стандарта IEEE 802.11ax.

4.3 Разработка рекомендаций по защите корпоративной сети стандарта IEEE 802.11ax.

4.4 Технико-экономическое обоснование предлагаемых мер по защите информации в беспроводной сети стандарта IEEE 802.11ax.

Приложение

Дата выдачи задания «04» апреля 2020 г.

Руководитель работы		В.Е. Рачков
	(*подпись*)	(*инициалы, фамилия*)
Консультанты по разделам		
	(*подпись*)	(*инициалы, фамилия*)
	(*подпись*)	(*инициалы, фамилия*)
	(*подпись*)	(*инициалы, фамилия*)
Задание к исполнению принял	«04» апреля 2020 г.	В.С. Заводнов
		подпись

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Институт информационных технологий и телекоммуникаций
Кафедра организации и технологии защиты информации
Направление подготовки Информационная безопасность
Направленность (профиль) Комплексная защита объектов информатизации

КАЛЕНДАРНЫЙ ПЛАН

Фамилия, имя, отчество Заводнов Вячеслав Сергеевич
Тема ВКР Анализ защищенности перспективной сети IEEE 802.11ax с обоснованием мер по ее защите
Руководитель Рачков В.Е.
Консультанты:

№	Наименование этапов выпускной квалификационной работы	Срок выполнения работы	Примечание
4.	Анализ литературы по теме работы	10.04.2020	
5.	Анализ системы управления компании и актуализация угроз информации	20.04.2020	
6.	Анализ защищенности перспективной сети стандарта IEEE 802.11ax.	22.05.2020	
7.	Разработка рекомендаций по защите корпоративной сети стандарта IEEE 802.11ax.	30.05.2020	
1.	Технико-экономическое обоснование предлагаемых мер по защите информации в беспроводной сети стандарта IEEE 802.11ax.	06.06.2020	
8.	Представление ВКР руководителю и нормоконтролеру	08.06.2020	
9.	Предварительная защита	10.06.2020	
10.	Представление ВКР заведующему кафедрой	19.06.2020	
11.	Рецензирование	23.06.2020	
12.	Представление ВКР в ГЭК	29.06.2020	

Руководитель В.Е. Рачков
Зав. кафедрой В.И. Петренко
«04» апреля 2020 г.

ПЕРЕЧЕНЬ ОБОЗНАЧЕНИЙ И СОКРАЩЕНИЙ

АРМ - Автоматизированное рабочее место

АС - Автоматизированная система

БД - База данных

ЗИ - Защита информации

ИА - Информационный актив

ИС - Информационная система

ИТС - Информационно-телекоммуникационная система

ИО - Информационное обеспечение

ИБ - Информационная безопасность

КСЗИ - Комплексная система защиты информации

ЛВС - Локальная вычислительная сеть

ОС - Организационная система

ОУ - Объект управления

ПО - Программное обеспечение

РД - Руководящий документ

СУБД - Система управления базами данных

СУ - Субъект управления

СЗИ - Система защиты информации

СУИБ - Система управления информационной безопасностью

ФСТЭК - Федеральная служба по техническому и экспертному контролю России

IoT – Internet of Things

Li-Fi - Технология беспроводной связи, схожая по принципу действия с Wi-Fi, но использующая видимый спектр (свет) в качестве канала для передачи информации

WAN – Глобальная сеть связи

WLAN – Беспроводная локальная сеть

WPA3 – Wi-Fi Protected Access 3

ВВЕДЕНИЕ

Развитие технологий беспроводной связи обуславливается отдельными тенденциями и драйверами, которые задают представление о потенциальном спросе и рыночных потребностях. Все это достаточно подробно анонсировано в национальной программе «Цифровая экономика РФ» [1] и детализировано в паспортах Федеральных проектов этой программы.

Анализ развития рынков информационных технологий показывает, что субтехнологии беспроводной связи WAN обеспечат рост рынка мобильных и носимых устройств за счет внедрения новых сервисов глобального уровня, таких как массовые машинные коммуникации и критически важные сервисы со сверхнизкой задержкой [2]. Также это обеспечит рост рынка и количества предоставляемых услуг за счет расширения возможностей коммуникации в разрезе увеличения пропускной способности мобильной сети и уменьшения задержек передачи информации. Прогнозируется, что субтехнологии WLAN расширят рынок устройств Wi-Fi внедрением нового протокола IEEE 802.11ax (Wi-Fi 6), а также создадут новый сегмент рынка устройств, поддерживающих технологию Li-Fi.

Выделенная субтехнология беспроводной связи на базе протокола IEEE 802.11ax обладает синергетическими эффектами с другими «сквозными» цифровыми технологиями. Более того, уже сегодня существует ряд проектов, подтверждающих важность взаимодействия вышеуказанных технологий. Так синергетический эффект технологии беспроводной связи может быть достигнут совместно со «сквозной» цифровой технологией «Новые производственные технологии» в части субтехнологии «Платформы промышленного интернета», в рамках которой беспроводная связь является базисом для построения сетей промышленного интернета, получения данных с датчиков и оборудования, а также обеспечивает массовые Интернет-коммуникации, в том числе за счет спутниковой связи. Дополнительно, беспроводная связь станет основой для создания полностью

автоматизированного производства на предприятиях с возможностью передачи необходимых объемов данных для локальных центров, что является потенциальной синергией с субтехнологией «Технологии «умного» производства». Также синергетический эффект технологии беспроводной связи может быть достигнут со «сквозной» цифровой технологией «Искусственный интеллект», так как беспроводная связь необходима для обеспечения более быстрой передачи больших объемов данных, требуемых для обучения алгоритмов искусственного интеллекта и принятия решений алгоритмами искусственного интеллекта, а также для автоматического управления такими потоками данных [1].

Активное использование беспроводных сетей нового поколения в условиях цифровой экономики потребует более высокого уровня информационной безопасности, что реализуется протоколом безопасности Wi-Fi Protected Access 3 (WPA3). WPA3 концентрируется на новых технологиях, которые должны закрыть щели, начавшие появляться в WPA2 и изменить подходы к контролю и администрированию таких сетей.

Актуальность работы определяется тем, что предложенные в ней рекомендации решают задачу снижения рисков потери информации в организации, использующей перспективную беспроводную сеть стандарта IEEE 802.11ax в интересах организации технологического процесса компании.

Научная новизна определяется тем, что разработанные на основе анализа стандарта IEEE 802.11ax рекомендации по защите информации в перспективной беспроводной сети могут стать основой для формирования процедур контроля и администрирования этих сетей.

Целью выпускной квалификационной работы является снижение рисков потери информации в организации, использующей перспективную беспроводную сеть стандарта IEEE 802.11ax.

Достижение цели работы реализуется через решение следующих задач:

1. Анализ системы управления компании и актуализация угроз

информации.

2. Анализ защищенности перспективной беспроводной сети стандарта IEEE 802.11ax.

3. Разработка рекомендаций по обеспечению защиты информации в беспроводной сети стандарта IEEE 802.11ax.

4. Технико-экономическое обоснование предлагаемых мер по защите информации в беспроводной сети.

Объектом выпускной квалификационной работы является интегрированная информационная система компании, обеспечивающая технологический процесс предоставления телекоммуникационных услуг и совместную работу пользователей в интересах обеспечения ключевых бизнес-процессов.

Предметом исследования выпускной квалификационной работы являются меры, обеспечивающие безопасное функционирование перспективной беспроводной сети на базе стандарта IEEE 802.11ax.

Практический результат работы связан с возможностью реализации разработанных рекомендаций по защите информации в конкретной телекоммуникационной компании ООО «Медиа-техника» г. Ставрополь, решающей задачи своей экономической стратегии в условиях конкуренции на рынке телекоммуникационных услуг.

1 Анализ системы управления компании и актуализация угроз информации

1.1 Характеристика телекоммуникационной компании

ООО «Медиа-техника» г. Ставрополь является юридическим лицом. Права юридического лица организация приобрела с даты ее государственной регистрации. ООО «Медиа-техника» зарегистрировано 9 июня 2008 года [3]. Регистратор – инспекция Федеральной налоговой службы по Промышленному району города Ставрополя.

Компания может иметь дочерние и зависимые общества. Компания вправе создавать свои филиалы и открывать представительства, как в Российской Федерации, так и за рубежом. Филиалы и представительства Компании не являются юридическими лицами и осуществляют свою деятельность от имени компании. Филиалы и представительства Компании действуют в соответствии с законодательством места нахождения филиала или представительства на основании положения о филиале.

Основными видами деятельности компании являются:

1. Деятельность в области радиовещания и телевидения.

2. Деятельность в области передачи (трансляции) и распространение программ телевидения и радиовещания.

3. Прочая деятельность в области электросвязи.

4. Услуги по производству развлекательных телевизионных программ, транслируемых в прямом эфире

5. Услуги по производству информационных радиопрограмм, транслируемых в прямом эфире.

6. Услуги по производству рекламно-коммерческих телевизионных программ, транслируемых в прямом эфире.

7. Услуги по производству развлекательных радиопрограмм, транслируемых в прямом эфире.

8. Услуги по производству прочих телевизионных программ, записываемых на магнитную ленту или другие технические носители информации для последующей трансляции.

9. Услуги по производству образовательных и просветительных радиопрограмм, записываемых на магнитную ленту или другие технические носители информации для последующей трансляции

10. Услуги по производству информационных телевизионных программ.

11. Услуги по производству образовательных и просветительных радиопрограмм, транслируемых в прямом эфире.

12. Услуги по производству информационных телевизионных программ, транслируемых в прямом эфире

13. Услуги по производству информационных радиопрограмм, записываемых на магнитную ленту или другие технические носители информации для последующей трансляции

Уставный капитал организации составляет 10 000 руб.

Для обеспечения деятельности Общества создаются следующие органы управления: общее собрание, единоличный исполнительный орган – директор.

Общество может иметь гражданские права и нести гражданские обязанности, необходимые для осуществления видов деятельности, не запрещенных федеральными законами и не противоречащих Уставу, может от своего имени приобретать и осуществлять имущественные и личные неимущественные права, нести обязанности, быть истцом и ответчиком в суде, арбитражном и третейском судах.

Общество является собственником имущества, переданного ему учредителями в качестве их вкладов, а также иного имущества, приобретенного и произведенного по допускаемым законом основаниям в процессе его деятельности. Общество осуществляет согласно действующему законодательству владение, пользование и распоряжение находящимся в его

собственности имуществом в соответствии с целями своей деятельности и назначением имущества.

Общество отвечает по своим обязательствам всем принадлежащим ему имуществом, на которое по действующему законодательству РФ может быть обращено взыскание. Общество не отвечает по обязательствам своих участников, по обязательствам РФ, субъектов РФ, муниципальных образований, равно как и последние не отвечают по обязательствам общества.

Общество имеет право в порядке, установленном действующим законодательством, самостоятельно осуществлять экспортно-импортные операции, необходимые для его уставной и хозяйственной деятельности.

Общество может создавать самостоятельно и совместно с другими предприятиями, учреждениями и организациями (независимо от их формы собственности и организационно-правовой формы) дочерние и зависимые хозяйственные общества с правом юридического лица, а также филиалы и представительства на территории РФ и за ее пределами, в том числе в иностранных государствах с соблюдением условий, установленных действующим на территории РФ законодательством и соответствующим законодательством иностранных государств. Филиалы и представительства являются обособленными подразделениями, расположенными вне места нахождения общества, представляют интересы общества, не являются юридическими лицами, действуют от имени общества на основании Положений, утверждаемых общим собранием участников общества.

Общество имеет круглую печать с полным фирменным наименованием на русском языке и указанием на место нахождения, а также может иметь штампы и бланки со своим наименованием, фирменное наименование, эмблему, товарный знак и другие реквизиты, регистрируемые в установленном законодательством порядке.

Общество может на добровольных началах объединяться в союзы и ассоциации, другие объединения на условиях, не противоречащих законодательству РФ.

Общество ведет бухгалтерский учет и отчетность в порядке, предусмотренном действующим законодательством.

Финансовый год общества совпадает с календарным годом.

Общество обязано хранить по месту нахождения его единоличного исполнительного органа или в ином месте, известном и доступном участникам общества, следующие документы:

– учредительные документы общество, а также внесенные в учредительные документы и зарегистрированные в установленном порядке изменения и дополнения;

– протоколы собрания учредителей общества, содержащие решения о создании общества и об утверждении денежной оценки неденежных вкладов в Уставный капитал, а также иные решения, связанные с созданием общества;

– документ, подтверждающий государственную регистрацию общества;

– документы, подтверждающие права общества на имущество, находящееся на его балансе;

– внутренние документы общества;

– положения о филиалах и представительствах общества;

– документы, связанные с эмиссией облигаций и иных эмиссионных ценных бумаг общества;

– протоколы общих собраний участников общества,

– заключения ревизора общества, аудитора, государственных и муниципальных органов финансового контроля;

– списки аффилированных лиц общества;

– иные документы, предусмотренные федеральными законами и иными правовыми актами РФ, Уставом, внутренними документами

общества, решениями общего собрания участников общества и исполнительного органа общества.

По требованию участника общества, аудитора или любого заинтересованного лица общество обязано в разумные сроки предоставить им возможность ознакомиться с учредительными документами, в том числе с их изменениями. Общество обязано по требованию участника общества предоставить ему копии действующего учредительного договора и устава общества. Плата за предоставление копий не может превышать затрат на их изготовление.

Руководство текущей деятельностью общества осуществляется единоличным исполнительным органом общества. Исполнительный орган подотчетен общему собранию участников общества.

Единоличным исполнительным органом общества является директор, который избирается общим собранием участников общества сроком на 1 год.

С директором заключается трудовой договор на срок 1 (Один) год. Со стороны общества трудовой договор подписывает председательствующий на общем собрании общества или участник общества, уполномоченный решением общего собрания участников общества.

Директор общества:

– без доверенности действует от имени общества, в том числе представляет его интересы и совершает сделки;

– осуществляет оперативное руководство работой общества;

– представляет на утверждение общего собрания участников проекты программ и планов хозяйственной деятельности общества, отчеты об их исполнении, в том числе годовой баланс и годовой отчет;

– созывает внеочередное и очередное общее собрание общества;

– инициирует созыв внеочередного общего собрания общества;

– выносит решение об отказе в созыве внеочередного общего собрания общества;

– включает вопросы в повестку дня внеочередного общего

собрания участников по собственной инициативе;

– организует ведение протокола на общем собрании общества;

– удостоверяет выписки из книги протоколов общего собрания общества, выдаваемых по требованию участников общества;

– имеет право первой подписи на документах общества, открывает в банках счета;

– выдает доверенности на право представительства от имени общества, в том числе доверенности с правом передоверия;

– заключает договоры и контракты от имени общества;

– разрабатывает и утверждает штатное расписание общества, принимает меры поощрения и взыскания в отношении работников, в соответствии с правилами внутреннего трудового распорядка;

– принимает и увольняет работников, в соответствии со штатным расписанием;

– издает приказы о назначении на должности работников общества, об их переводе и увольнении, применяет меры поощрения и налагает дисциплинарные взыскания;

– представляет на утверждение общего собрания участников кандидатуру своих заместителей.

Общество вправе передать по договору полномочия директора управляющему. Договор с управляющим подписывается от имени общества лицом, председательствовавшим на общем собрании участников общества, утвердившем условия договора с управляющим, или участником общества, уполномоченным решением общего собрания участников общества.

1.2 Анализ системы управления компании

Система управления – это совокупность всех элементов, подсистем и коммуникаций между ними, а также процессов, обеспечивающих заданное (целенаправленное) функционирование организации [4]. Организационная

структура ООО «Медиа-техника» [3], отражает состав структурных подразделений и определяет координацию их совместной деятельности на пути достижения поставленных перед компанией целей.

Директор осуществляет руководство деятельностью компании и обеспечивает эффективное взаимодействие структурных подразделений между собой, обеспечивает выполнение заданий согласно установленным количественным и качественным показателям, организует производственно - хозяйственную деятельность на основе применения методов научно обоснованного планирования материальных, финансовых и трудовых затрат, максимальной мобилизации резервов производства. Кроме этого директор решает все вопросы в пределах предоставленных прав и поручает выполнение отдельных производственно - хозяйственных функций другим должностным лицам компании (рисунок 1.1).

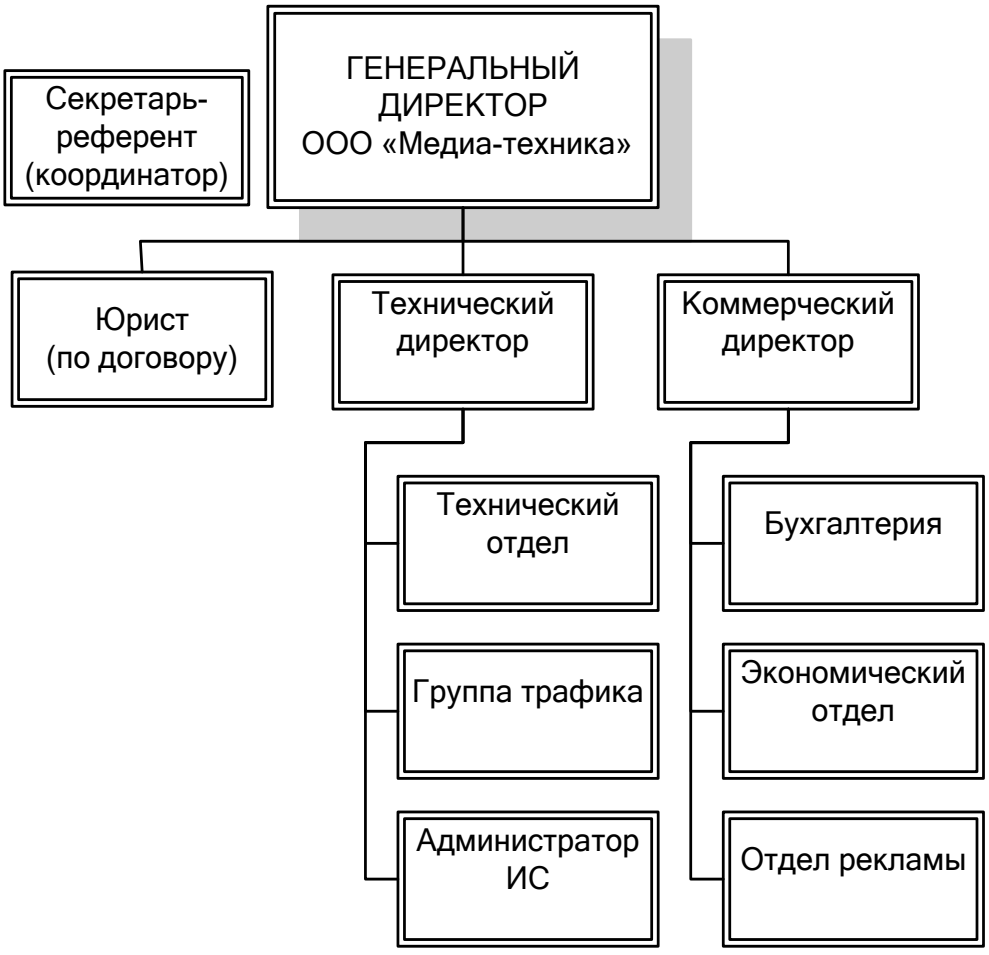

Рисунок 1.1 - Организационная структура ООО «Медиа-техника»

Сфера деятельности секретаря-референта связана с решениями задач организационного и документационного обеспечения управленческой деятельности в компании, а также с решениями задач кадрового менеджмента.

Организацию бухгалтерского учета и финансовой деятельности компании и контроль за использованием материальных и финансовых ресурсов, сохранностью собственности организации осуществляет бухгалтерия. Бухгалтерия организует учет поступающих денежных средств, товарно-материальных ценностей и основных средств, своевременное отражение на счетах бухгалтерского учета операций, связанных с их движением, учет издержек производства и обращения, исполнения смет расходов, реализации продукции, выполнения услуг, результатов финансовой деятельности представительства компании, а также финансовых, расчетных и кредитных операций. Обеспечивает контроль: за законностью, своевременностью и правильностью оформления документов; составлением экономически обоснованных отчетных калькуляций себестоимости продукции, услуг; расчетами по заработной плате с работниками компании; правильным начислением и перечислением платежей в государственный бюджет, взносов на государственное социальное страхование, средств на финансирование капитальных вложений; погашением в установленные сроки задолженностей банкам по ссудам; отчислением средств в фонды экономического стимулирования и другие фонды и резервы. Принимает меры по предупреждению недостач, незаконного расходования денежных средств и товарно-материальных ценностей, нарушений финансового и хозяйственного законодательства. Ведет работу по обеспечению строгого соблюдения штатной, финансовой и кассовой дисциплины, смет административно - хозяйственных и других расходов, законности списания с бухгалтерских балансов недостач, дебиторской задолженности и других потерь, сохранности бухгалтерских документов, а также оформлению и сдаче их в установленном порядке в архив.

Экономический отдел является самостоятельным структурным подразделением компании. В большинстве случаев экономический отдел подчиняется непосредственно коммерческому директору. Состав и штатную численность экономического отдела утверждает Генеральный директор компании исходя из условий и особенностей деятельности компании. Экономический отдел осуществляет:

– формирование ценовой и экономической политики компании на основании действующих нормативных актов и внутренних документов компании,

– формирование финансового плана (бизнес-плана) развития компании, контроль за ходом его выполнения, организацию ведения статистической отчетности в компании, увязанной с экономическими показателями развития,

– проведение экономического анализа финансово-хозяйственной деятельности компании,

– анализ состава затрат при формировании цен на услуги и сервисы компании,

– контроль соблюдения государственной финансовой дисциплины при заключении договоров и осуществлении экономической и хозяйственной деятельности компании,

– внутренний финансовый контроль за правильностью применения цен (тарифов) на услуги, оказываемые компанией,

– оформление служебных командировок работников компаний,

– разработка сметной документации.

Отдел рекламы это творческая часть компании, создающая источники информации, позволяющие населению узнать, и познакомится с конкретными услугами и сервисами компании. Отдел рекламы реализует следующие задачи:

– реализация рекламы услуг и сервисов, с целью увеличения количества продаж,

– создание рекламного проекта, который заинтересует аудиторию и повлечет в благоприятное русло для компании,

– изучение сервисов и услуг конкурентов, для создания эффективных методов продаж и акций,

– изучение статистки, с помощью которой можно подобрать подходящее место для распространения информации,

– оформление: стиль, музыкальное сопровождение, цветовые гаммы,

– изобретение собственного, неповторяющегося стиля предприятия,

– формирование выставочных стендов,

– оформление приглашений,

– определения сроков проведения мероприятий,

– подписания соглашений, о проведении рекламы с источниками информации,

– расширение потребительского рынка компании,

– изучение реклам конкурентов, для усовершенствования своей деятельности,

– проведение опросов и составление статистики по рекламе,

– учет расходов.

Администрирование технологической локальной сети осуществляет один из системных администраторов технического отдела. Так же в его должностные обязанности входит установка и поддержка программного обеспечения, обучение персонала основным навыкам работы вычислительной техникой и оборудованием, приложениями, диагностика и ремонт оргтехники офиса, проведение мероприятий по обеспечению информационной безопасности компании.

Технический отдел является основным и самостоятельным структурным подразделением компании, решающим задачи с обеспечения

предоставления телекоммуникационных услуг, технологическое сопровождение основных бизнес-процессов.

1.3 Цели и задачи компании на телекоммуникационном рынке

Под целью понимается информационный образ желаемого состояния или результата деятельности. Точная формулировка и определение целей ООО «Медиа-техника» облегчает выбор средств их достижения. Поэтому определение целей системы является важным этапом в процессе формирования и принятия решений.

Выявление целей проводится на основе системного анализа. Каждая система имеет множество согласованных между собой целей, которые должны работать на главную цель.

Обычно цели задаются в виде некоторых общих целевых установок для системы в целом. Такая постановка целей делает необходимой дальнейшую детализацию и конкретизацию целей по мере продвижения вниз по организационным уровням управления. Решением проблемы является декомпозиция сложных целей с помощью методики построения дерева целей на основе системного подхода. Система достигает главной цели через достижение целей элементами, ее составляющими.

Содержательная формулировка целей является необходимым, но недостаточным условием осуществления целеполагания. Для конкретизации целей необходимо задать критерии достижения целей и ограничения, в рамках которых осуществляется поиск возможных вариантов решения.

Критерий достижения цели отождествляется с показателем эффективности системы и выступает как измеритель степени достижения намеченной цели. Внутри критерия должен присутствовать числовой показатель, по которому осуществляется оценка критерия.

Главной целью ООО «Медиа-техника» является получение прибыли. Критерием достижения главной цели является объем прибыли, получаемой ООО «Медиа-техника» за некоторый фиксированный период времени.

Список целей и средств их достижения для ООО «Медиа-техника» приводится в таблице 1.1.

Таблица 1.1 — Цели, стоящие перед компанией

Цель	Средства или принципы ее достижения	Критерий (показатель) эффективности
Увеличение доли рынка телекоммуникационных услуг.	Применение информационно-аналитических средств маркетинга. Проведение PR-компаний.	Увеличение объемов продаж сервисов и услуг.
Достижение лидирующих позиций на рынке информационных сервисов.	Увеличение ассортимента телекоммуникационных услуг. Проведение рекламной кампании. Повышение цитируемости портала компании. Оптимизация политики цен. Удовлетворение информационных потребностей клиентов.	Объем продаж в единицу времени.
Постоянное совершенствование качества обслуживания клиентов	Повышение требований к сотрудникам организации по качеству обслуживания. Проведение проверок методом «тайный покупатель».	Увеличение числа клиентов. Наработка постоянных клиентов. Удержание клиентов.
Получение максимальной прибыли от торговли	Повышение качества финансового анализа деятельности компании. Материальная и моральная мотивация специалистов.	Увеличение притока денежных средств.

1.4 Проблемности в области обработки информации

Важным этапом принятия решения по вопросам защиты информации, является выделение проблем связанных с угрозами информации. Проблемная ситуация возникает всякий раз, когда имеет место расхождение между желаемым и реальным состоянием системы

(процесса, объекта) [5]. Решение же принимается для ликвидации проблемной ситуации.

Формулировка проблемы является наиболее важной ступенью в решениях самой проблемы. Правильно сформулированная проблема, может считаться наполовину решенной. Сформулированная проблема может привести к возникновению новых проблем при попытке ее разрешения.

Если проблема глобальна, то она первична и порождает главную цель системы. Если система находится в достаточно стабильном состоянии, то есть функционирует без кризисов и сбоев, то цели, стоящие перед системой, порождают проблемные ситуации. Оценка проблемных моментов, присутствующих в организации, дает возможность провести актуализацию мер по их устранению или же минимизации. Под угрозой безопасности информационной системы компании понимают возможность воздействия на нее, которое прямо или косвенно может нанести ущерб ее безопасности. С этой целью необходимо классифицировать угрозы безопасности. Невозможно формализовать задачу без описания полного множества угроз. Для компании ИС является основой для реализации экономической стратегии, поэтому классификация должна быть реализована по аспекту информационной безопасности (доступность, целостность, конфиденциальность).

Самые частые проблемы при работе с информацией на любом производстве связаны с вирусами. Сотрудники вносят вирусы при установке программ, посещении зловредных сайтов. Утечка информации может быть связана с работой вирусов, которые перехватывают пароли, причем они могут заблокировать систему или действовать в тихом режиме.

Список проблемных ситуаций представлен в таблице 1.2. Основной проблемой для ООО «Медиа-техника» является недостаточно

эффективная работа с клиентами компании, т.к. именно они являются заказчиками рекламных услуг и основным источником дохода компании.

Таблица 1.2 - Перечень проблемностей в области защиты информации

№	Формулировка проблемы	Способы ее решения
1	2	3
1.	Нехватка финансовых средств и несовершенство управления активами компании	1.1.Выпуск акций. 1.2. Расширение сети представительств. 1.3. Привлечение и обучение высокопрофессиональных кадров для работы на финансовых рынках.
2.	Низкая оперативность принятия решений в условиях неопределенности.	2.1. Внедрение автоматизированных аналитических систем. 2.2 Создание автоматизированных рабочих мест для специалистов. 2.3 Улучшение условий труда.
3.	Нехватка высокопрофессиональных специалистов	3.1.Обучение имеющихся кадров. 3.2.Привлечение новых специалистов методами стимулирования. 3.3.Создание спецкурсов для обучения новых специалистов.
4.	Недостаточно эффективная система защиты информации в компании	4.1 Внедрение автоматизированных аналитических и информационно-справочных систем администрирования. 4.2.Привлечение квалифицированных кадров. 4.3.Финансирование обучения и повышения квалификации. 4.4.Широкое использование ресурсов сети Internet, кабельного телевидения, своевременная закупка литературы, разработка и издание собственных узкоспециализированных электронных пособий. 4.5 Регламентирование деятельности администратора информационной системы и должностных лиц службы информационной безопасности по снижению рисков потери информации в информационной системе.
5	Угрозы потери критически важной для компании информации и данных	5.1 Анализ угроз, уязвимостей и рисков в информационной среде компании. 5.2 Разработка модели угроз информационной безопасности компании. 5.3 Развертывание и совершенствование системы защиты информации компании. 5.4 Реализация процедур внутреннего и внешнего аудита информационной безопасности. 5.5 Совершенствование системы администрирования сетей передачи данных (беспроводных сетей).

В каждой организации существует защищаемая информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Данная информация подразделяется на общедоступную информацию и информацию ограниченного доступа. К общедоступной информации относятся общеизвестные сведения и иная информация, доступ к которой не ограничен. К информации ограниченного доступа относится информация, доступ к которой ограничен в соответствии с федеральными законами. К данной категории, в рамках удостоверяющего центра, попадает информация, составляющая служебную тайну, а также персональные данные.

К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью [6].

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

В ООО «Медиа-техника» можно выделить следующие защищаемые информационные активы [1]:

- ключ электронной подписи,
- ключ проверки электронной подписи,
- сертификат ключа проверки электронной подписи,
- персональные данные сотрудников,
- персональные данные клиентов,
- иные сведения клиентской базы данных (общие клиентские сведения, сведения об отправленной отчетности, сведения о предоставляемых клиенту услугах),
- сведения из документации в области технологий вещания,
- клиентская документация,

- нормативная документация организации (регламент работ по оказанию услуг, регламент работы организации, инструкция по установке ПО и т.п.),
- копии договоров с клиентами, хранящиеся в архивном фонде компании,
- сведения об оплате услуг.

Так же к защищаемым активам предприятия относятся ресурсы. К защищаемым ресурсам ООО «Медиа-техника» относятся:

- аппаратные средства, входящие в среду вещания,
- программные компоненты среды вещания,
- каталоги и файлы с конфиденциальной информацией,
- системные программные средства, средства операционной системы,
- персонал, обрабатывающий сведения, подлежащие защите,
- средства обработки защищаемой информации,
- съемные носители: магнитные диски, оптические диски, флеш-накопители, защищенные накопители eToken,
- специализированные прикладные программные средства,
- сервер для хранения и обработки клиентской базы данных.

Учитывая специфику обрабатываемой информации и используемые средства для ее обработки, можно выделить следующие основные объекты и среды, по которым наиболее вероятны реализации угроз в ООО «Медиа-техника»:

- помещения, в которых находится совокупность программных и технических элементов систем обработки данных и средства электронной подписи,
- сетевые серверы и средства,
- каналы связи и сети передачи данных,
- персонал.

Через смежные помещения могут быть реализованы следующие угрозы:

- перехват информации, обрабатываемой в защищаемых технических средствах, за счет побочных электромагнитных излучений и наводок, выходящих за пределы контролируемой зоны,
- прослушивание акустической информации за счет внедрения закладных устройств,
- перехват акустической информации с использованием направленных микрофонов,
- перехват акустической информации за счет оптического канала утечки информации,
- перехват акустической информации за счет виброакустического канала утечки информации (с использованием стетоскопов).

Утечка информации через сетевые средства реализуется за счет:

- анализа злоумышленником сетевого трафика,
- сканирования сети и его беспроводного сегмента,
- угрозы утраты ключей и атрибутов доступа,
- отказа в обслуживании (DDOS-атаки),
- угрозы подмены доверенного объекта в сети,
- MAC-спуфинга,
- ARP-спуфинга,
- порчи оборудования,
- внедрения вирусов, вредоносных программ и прочее.

Так же возможна реализация следующих угроз через линии связи и сети передачи данных:

- прослушивание информации, циркулирующей в линии связи, за счет внедрения закладных устройств,
- прослушивание информации, циркулирующей в линии связи, за счет микрофонного эффекта акустоэлектрических преобразователей,

- прослушивание информации, циркулирующей в линии связи, за счет параллельного подключения к линии,
- съем информации циркулирующей в беспроводных сетях,
- повреждение каналов связи.

Последними, но немаловажными угрозами являются угрозы утечки информации через персонал:

- намеренное или случайное разглашение информации,
- не соблюдение правил обработки защищаемой информации,
- разглашение защищаемой информации,
- ошибочные или случайные действия лицами, взаимодействующими с информационными ресурсами в рамках своих полномочий,
- сотрудничество со злоумышленниками,
- подкуп или шантаж со стороны третьих лиц,
- допуск к конфиденциальным сведениям посторонних лиц,
- кража списанных носителей информации,
- копирование защищаемой информации,
- разглашение ключевой информации для доступа к защищаемым данным.

1.5 Выводы по разделу

1. Компания реализует предоставление услуг в медиа пространстве и имеет сложную, распределенную технологическую и информационную инфраструктуру. Созданная информационная инфраструктура обеспечивает решение как управленческих, так и технологических задач.

2. Критически важными информационными активами компании, представляющими наибольший интерес для злоумышленников и конкурентов, являются:

– бизнес-план компании,

- счета фактуры и другие финансовые документы,
- особенности аппаратного, программного обеспечения и информационной инфраструктуры,
- ключ электронной подписи, ключ проверки электронной подписи, сертификат ключа проверки электронной подписи,
- персональные данные сотрудников, персональные данные клиентов, иные сведения клиентской базы данных (общие клиентские сведения, сведения об отправленной отчетности, сведения о предоставляемых клиенту услугах).

3. Для решения задач предоставления телекоммуникационных услуг и сервисов в компании создана организационно-штатная структура. Особенности информационных технологий работы с информацией связаны с одновременным использованием как информационной, так и технологической системами.

4. Как показала организационно-штатная структура, отдельного структурного подразделения, отвечающего за защиту информации нет. Эта задача возложена на администратора.

5. В компании в интересах управления технологическими операциями и внутриорганизационным обменом данными используется интегрированная информационная система с постоянной динамикой увеличения трафика и объема передаваемых данных.

6. Имеет место потребность перехода на сетевые технологии, в том числе беспроводной передачи данных, с возможностями передачи большого объема информации и высокими скоростями. Такие возможности предоставляют беспроводные сети, функционирующие на базе перспективного протокола IEEE 802.11ax с встроенным механизмом защиты WPA3, которые требуют совершенствования процедур администрирования в интересах защиты информации, циркулирующей в этих сетях.

2 Анализ защищенности перспективной сети стандарта IEEE 802.11ax

2.1 Общая характеристика стандарта IEEE 802.11ax

Причиной эволюции Wi-Fi стал и такой важный тренд как «интернет вещей» (Internet of Things - IoT), который представляет собой серьезную проблему для организаций. Ведь важным является проблема безопасного и простого подключения сотен или более электронных устройств к корпоративной информационной системе в соответствии с их эксплуатационными и инженерными потребностями. В отличие от пользовательских устройств, таких как ноутбуки, IoT-устройства нуждаются либо в детерминированном беспроводном обслуживании, либо в сервисе с низким энергопотреблением. Традиционно эти потребности удовлетворялись с помощью запатентованной, брендовой технологией или технологией, специфичной для поставщика беспроводных услуг. Но корпоративный Wi-Fi все чаще выбирался в качестве внутренней платформы IoT из-за значительной экономии за счет масштаба и простоты управления со стороны ИТ-инфраструктуры. И для удовлетворения этих эксплуатационных потребностей IoT, 802.11ax может стать основой платформы для передачи беспроводных данных.

В мире активно используется большое количество устройств Wi-Fi - примерно на 9 миллиардов больше чем людей [7]. Это активное распространение делает защиту Wi-Fi от хакеров одной из самых важных задач в области информационной безопасности. Именно поэтому появление протокола беспроводной безопасности следующего поколения WPA3 является важным, поскольку он не только обеспечит безопасность соединений Wi-Fi, но и помогает избавиться от корпоративных уязвимостей в области информационной безопасности.

16 сентября 2019 года была принята сертификационная программа Wi-Fi Alliance - Wi-Fi 6, которая, как предполагается, должна обеспечить эффективную работу пользователей с устройствами на основе стандартов IEEE 802.11ax [8]. Эта программа сертификации принесла новые функции и возможности, которые позволяют существенно увеличить общую производительность Wi-Fi-устройств с большим количеством подключений. Wi-Fi 6 отвечает требованиям к безопасности и совместимости с более ранними версиями стандарта 802.11. Новая версия Wi-Fi обеспечивает значительную емкость, производительность и сокращение задержек всей беспроводной экосистемы, обеспечивая хорошую совместимость вне зависимости от производителя оборудования.

Wi-Fi 6 поддерживает большой набор устройств и приложений. Среди них и те, которым необходима максимальная производительность в требовательных корпоративных средах с низким энергопотреблением и низкой задержкой в «умных» домах или сценариях промышленного «интернета вещей». Благодаря высокой скорости, низкой задержке, энергоэффективности, увеличенной пропускной способности и расширения радиуса действия, новые Wi-Fi-устройства смогут предоставить множество дополнительных услуг. Wi-Fi 6 поддерживает современные протоколы безопасности и обеспечивает безопасность Wi-Fi последнего поколения по стандарту WPA3.

IEEE 802.11ax имеет следующие технические характеристики [8]:

1. Множественный доступ с ортогональным частотным разделением (OFDMA): позволяет разделять каналы для повышения эффективности сети и сокращения времени ожидания как для исходящего, так и входящего трафика в высоконагруженных средах/

2. Многопользовательский множественный ввод - множественный вывод (MU-MIMO): позволяет передавать данные на большее количество устройств одновременно.

3. Каналы шириной 160 МГц: увеличивают пропускную способность, обеспечивают более высокую производительность с низкой задержкой.

4. Целевое время пробуждения (TWT): значительно увеличивает срок службы источников питания Wi-Fi-устройств, таких как устройства «интернета вещей» (IoT).

5. Реализуется 1024-квадратурная амплитудная модуляции (1024-QAM): увеличивает пропускную способность в сети Wi-Fi-устройств, позволяет кодировать больше данных в той же ширине спектра.

6. Автоматическое формирование диаграммы направленности (beamforming): обеспечивает более высокую скорость передачи данных в заданном радиусе действия, что приводит к большей пропускной способности сети.

2.2 Характеристика технических решений стандарта IEEE 802.11ax

В ходе эволюции стандартов сетей Wi-Fi скорость передачи данных увеличивается за счет использования частотных ресурсов. Например, ширина канала увеличивалась от 20 МГц в первых версиях стандарта до 160 МГц в 802.11ac. Та же тенденция наблюдалась и с уровнями модуляции, и с количеством потоков MIMO. В момент перехода с 802.11n на 802.11ac у многих экспертов сложилось впечатление [7], что предел разработок достигнут, ведь при переходе на 802.11ac ничего существенного не произошло: просто увеличили число антенн и ширину полосы частот. Однако 802.11ax привнес множество изменений, которые позволят использовать спектр более эффективно. К этим технологиям можно отнести:

- OFDMA,
- Resource Units,
- Target Wait Time (TWT),
- BSS coloring.

Множественный доступ с ортогональным частотным разделением (OFDMA) - это возможность выделения ресурсного блока в том же PPDU (Physical layer Protocol Data Unit - блок данных протокола физического уровня) каждому клиенту или станции (STA). Несмотря на то, что OFDMA-технология не новая, она является уникальной для 802.11ax в семействе 802.11. С самым малым блоком ресурса может быть 26 поднесущих (2 МГц) и с самым большим - 2 x 996 поднесущих (160 МГц) (Рисунок 2.1).

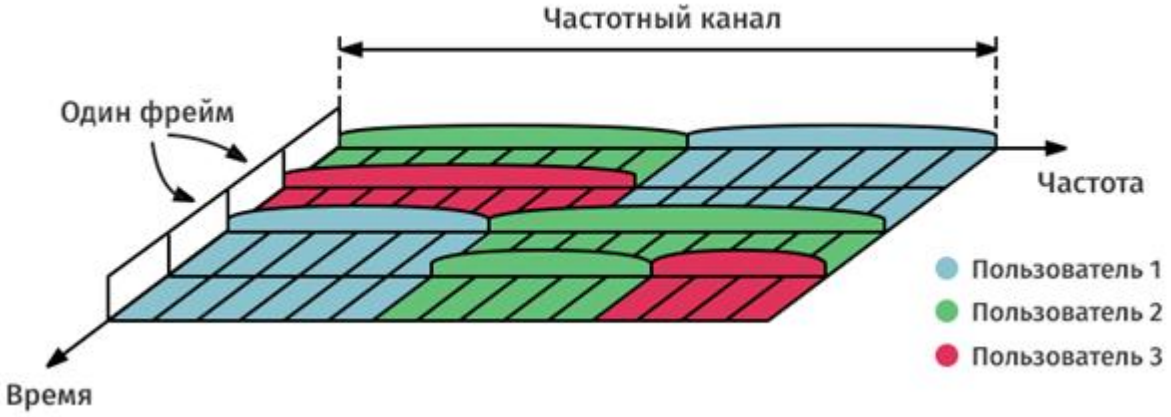

Рисунок 2.1 – Реализация множественного доступа с ортогональным частотным разделением

В 802.11ac технология MIMO (Multiple Input Multiple Output) позволяла транслировать данные четырем клиентам с помощью разных поднесущих. В 802.11ax число возможных подключений устройств увеличили в два раза.

В отличие от 802.11ac, оборудование 802.11ax может управлять распределением ресурсов нисходящей и восходящей линий связи на основе PPDU, что можно рассматривать как способ радиопланирования точек доступа в частотной и пространственной областях.

Хоть 802.11ax не использует радиопланирование на основе времени, аналогичное стандарту LTE, можно представить, что для достижения аналогичных результатов в качестве сотовой связи используются передовые методы организации очередей или QoS, поскольку базовая структура уже существует, и чистая сеть 802.11ax будет иметь отличные возможности управления спектром и помехами.

Канал OFDMA 20 МГц состоит в общей сложности из 256 поднесущих (тонов). Эти тона сгруппированы в более мелкие подканалы, известные как Resource Units (RUs). При разделении канала на 20 МГц точка доступа 802.11ax обозначает как 26, 52, 106 и 242 единицы ресурса поднесущей (RUs), что примерно соответствует каналам 2 МГц, 4 МГц, 8 МГц и 20 МГц соответственно (Рисунок 2.2). Точка доступа 802.11ax определяет, сколько поднесущих используется в канале 20 МГц, и может использовать различные комбинации этих поднесущих при передачи данных.

Рисунок 2.2 - Единицы ресурса поднесущей стандарта

Точка доступа 802.11ax может выделить весь канал одному клиенту в один момент времени, или разделить канал OFDMA таким образом, чтобы он мог использоваться несколькими клиентами. Например, точка доступа 802.11ax может взаимодействовать с одним клиентом, используя 8 МГц частотного пространства, а также с тремя дополнительными клиентами используя 4 МГц субканалов.

В предыдущих поколениях семейства 802.11 маломощные устройства, такие как мобильные телефоны, обеспечивали автоматическое энергосбережение (U-APSD) или Wi-Fi Multi Media Power-Save (WMM-PS).

Точка доступа осуществляла буферную передачу, а не немедленную доставку данных. Другими словами, точка доступа сигнализировала о наличии данных в специальных пакетах, через сообщение индикации трафика (TIM), что позволяло клиенту сохранять свой радиоприемник выключенным (экономия энергии) и возобновляет только периодически для приема маяков (обычно кратно каждые 102,4 МС). Однако, это строгое соблюдение маяков ограничивает потенциал энергосбережения для устройств IoT, которые не требуют регулярного доступа к каналу, как мобильный телефон, но всегда должны быть готовы принять телефонный звонок.

С TWT больше не существует тесной связи между маяками точек доступа и временем сна устройства (Рисунок 2.3). Как правило, станция может запросить расписание, чтобы проснуться в любое время в будущем. Результатом является значительная экономия энергии для устройств с батарейным питанием, особенно в пространстве IoT-систем.

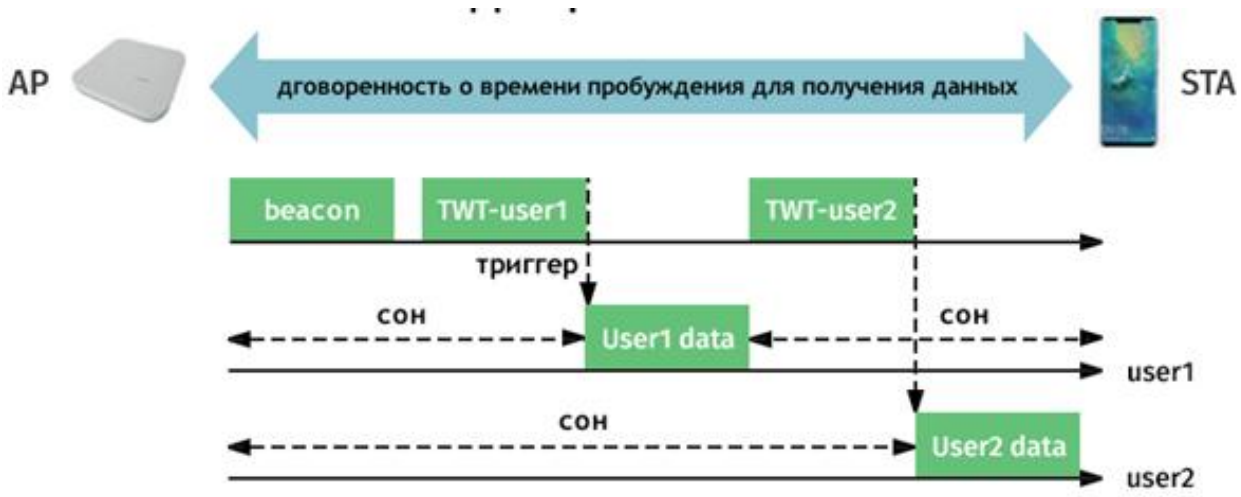

Рисунок 2.3 – Диаграмма времени ожидания цели

Поскольку TWT эффективно переводит клиентов в спящий режим с заданным временем пробуждения (на основе их запроса), возможно детерминированное время передачи и, следовательно, планирование приёма данных оконечным устройством. Точка доступа может использовать эту возможность как для уменьшения конкуренции (более распределенного

использования каналов), так и для устранения чувствительности приложений к задержке.

С любой беспроводной системой, включая сети на основе 802.11 CSMA (Carrier Sense Multiple Access - множественный доступ с прослушиванием несущей), совместное использование одного и того же радиочастотного канала в одном и том же физическом пространстве всегда было проблемой.

Критически важно, что уровень сигнала (RSSI), на котором точка доступа использует канал, является «свободным для передачи» или то, что мы называем Carrier Sense (CS). Однако в дальнейшем, 802.11ax стандартизирует это поведение для обеспечения оптимального улучшения производительности.

BSS Color – это метод для разделения BSSs - то есть точек доступа и их клиентов на одном и том же радиочастотном канале.

Работа BSS Color заключается в следующем (Рисунок 2.4):

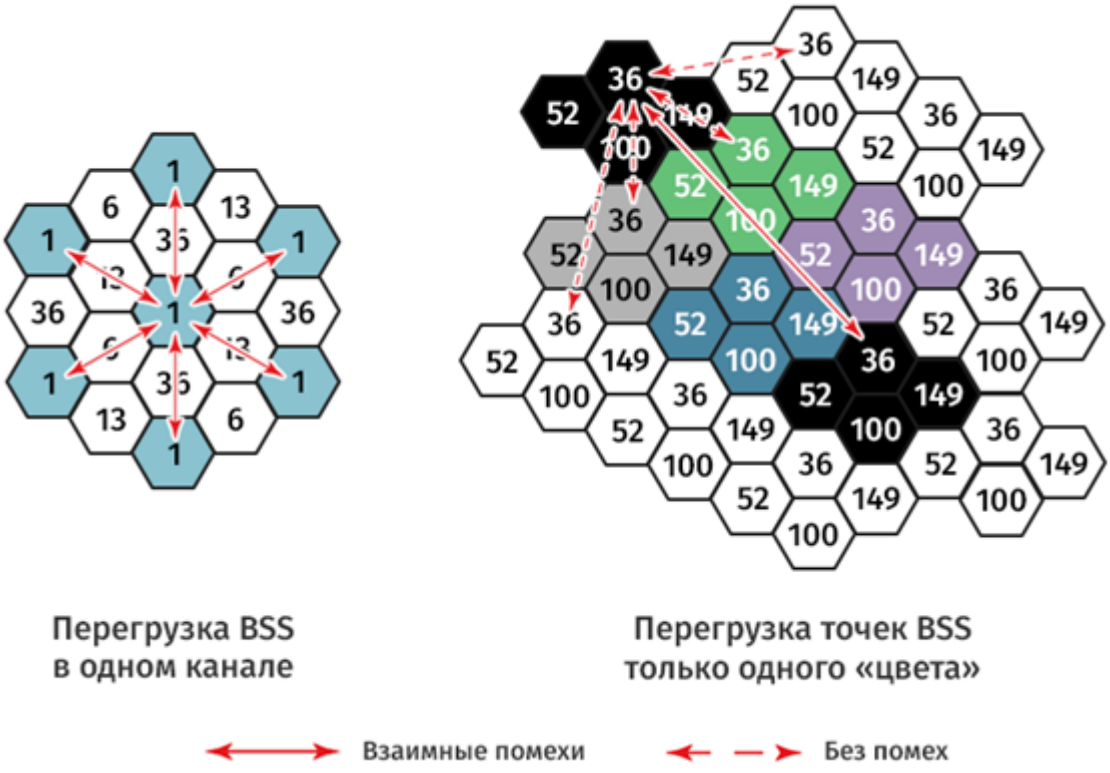

Рисунок 2.4 – Работа BSS coloring

1. Каждый BSS - точка доступа использует другой «цвет» (6 бит в преамбуле сигнала или SIG).

2. Сигналы с тем же цветом BSS используют низкий порог RSSI для отсрочки, тем самым уменьшая столкновения в той же зоне обслуживания.

3. Сигналы с другим цветом BSS используют более высокий порог RSSI для отсрочки, тем самым обеспечивая большее количество одновременных передач.

Таким образом, этот метод используется для улучшения сосуществования перекрывающихся источников сигнала, уменьшения коллизий и для обеспечения возможности повторного использования пространства в одном канале. Это означает, что окрашивание BSS помогает в смягчении проблемы помех в канале, обнаруженных в устаревших сетях Wi-Fi.

Важным является то, что стандарт 802.11ax не вызывает проблем совместимости с уже созданной беспроводной инфраструктурой, так как 11ax имеет обратную совместимость с ранее выпущенными стандартами Wi-Fi - 802.11a / g / n / ac. Для этого точки доступа 802.11ax используют свой определенный формат PPDU для взаимодействия с клиентами каждого из перечисленных форматов.

Новая технология Wi-Fi поддерживает до 8 SS и обеспечивает скорости передачи данных в 600–1800 Мбит/с для клиентов (с 1024 QAM). Ожидается, что клиенты, поддерживающие стандарт 802.11ax, будут доступны в большом количестве уже в конце 2019, начале 2020 года. IEEE 802.11ax обеспечит [8]:

– передачу видео в формате 4K/8K для нескольких пользователей одновременно,

– поддержку клиентов в высоконагруженных хот-спотах (Ultra-High-Density - UHD),

– детерминизм для приложений AR/VR и значительная экономия энергии, особенно для устройств IoT.

Критически важные приложения все чаще требуют детерминизма и предсказуемости в обслуживании. Другими словами, для обеспечение

высоких показателей качества обслуживания, оборудование должно обладать информацией о времени передачи пакетов. Новый стандарт Wi-Fi 6 802.11ax обладает всеми необходимыми технологическими решениями для предоставления качественного беспроводного соединения для IoT и VR-устройств.

2.3 Характеристика механизмов защиты стандарта IEEE 802.11ax

Wi-Fi Alliance [7] обнародовал крупнейшее обновление безопасности Wi-Fi за последние 16 лет. Протокол безопасности Wi-Fi Protected Access 3 (WPA3) вводит очень нужные обновления в предыдущий протокол WPA2, представленный еще в 2004 году. WPA3 концентрируется совершенно на новых технологиях, которые должны устранить уязвимости, начавшие появляться в WPA2. Wi-Fi Alliance также объявил о двух дополнительных, отдельных протоколах сертификации, вводящихся в строй параллельно WPA3 [8]. Протоколы Enhanced Open и Easy Connect не зависят от WPA3, но улучшают безопасность для определённых типов сетей и ситуаций.

2.3.1 Процедура одновременной аутентификации

Важнейшее изменение которое принесёт WPA3 - это новый метод аутентификации устройств в сети. Самый главный момент в защите сети наступает, когда новое устройство пытается установить соединение. Злоумышленник должен оставаться за пределами, поэтому WPA2 и WPA3 уделяют много внимания аутентификации новых соединений и гарантии того, что они не будут являться попытками хакера получить доступ.

SAE (Simultaneous Authentication of Equals) – новый метод аутентификации устройства, пытающегося подключиться к сети. SAE – это вариант т.н. dragonfly handshake - установления связи по методу «стрекозы», использующего криптографию для предотвращения угадывания пароля

злоумышленником. Он говорит о том, как именно новое устройство, или пользователь, должен «приветствовать» сетевой маршрутизатор при обмене криптографическими ключами (Рисунок 2.5).

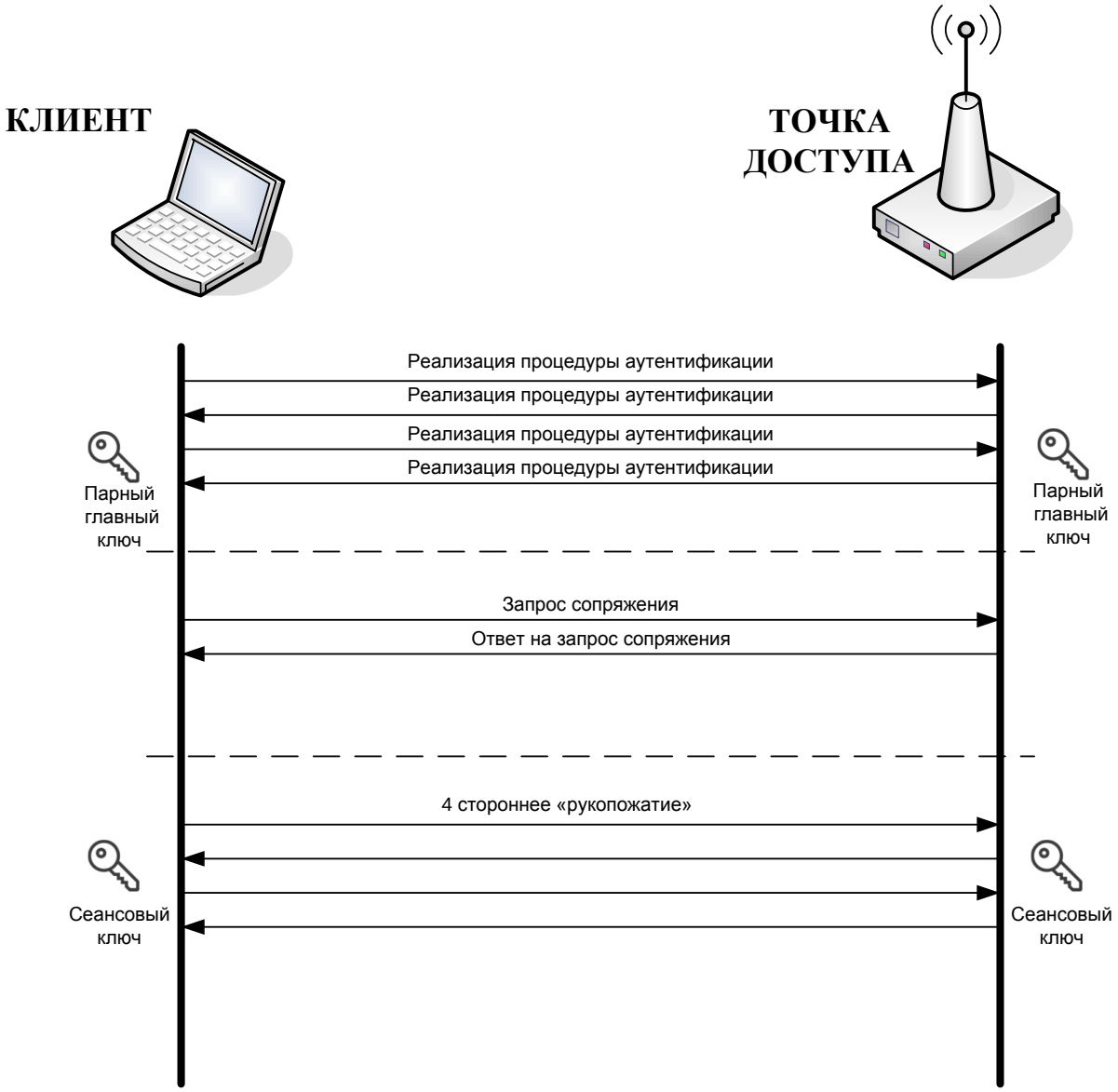

Рисунок 2.5 – Процедура реализации SAE

Протокол SAE - это вариант Dragonfly, который предусматривает обмен ключами на основе доказательства с нулевым разглашением , поэтому пароль фактически не обменивается. Концепция та же самая, что лежит в основе каждого протокола для обмена ключами: оба субъекта проходят проверку подлинности с использованием общего секрета (например, пароля),

и в итоге будет секретный объект, который можно использовать при обмене данными между двумя абонентами.

SAE может использоваться различными клиентами для аутентификации и создания ключа сеанса и поддерживает криптографию конечного поля (FFF) и криптографию с эллиптической кривой (ECC), при этом по умолчанию используется ECC. После обмена с SAE генерируется один парный главный ключ (PMK), общий для клиента и точки доступа. После создания PMK процесс сопряжения завершается, и 4-стороннее взаимодействие начинает создавать сеансовый ключ.

С точки зрения безопасности, SAE - это протокол, который противостоит как пассивным, так и активным атакам, атакам по словарю и повторным атакам. В частности:

– пассивные атаки, когда злоумышленник просто передает трафик между двумя законными субъектами, пытаясь извлечь из сообщений полезную информацию (пароль или общий ключ), невозможен. То же самое относится и к активным атакам, когда злоумышленник вмешивается непосредственно в сообщения, модифицируя их,

– атака по словарю неэффективна, поскольку у злоумышленника нет возможности проверить гипотезу, то есть, если пароль неверен, протокол должен быть перезапущен с использованием другой гипотезы и т. д. Таким образом, злоумышленник не может выполнить атаку и повторять попытки офлайн, пока не найдет правильный пароль,

– протокол реализует прямую секретность, то есть даже знание долгосрочного ключа шифрования не дает злоумышленнику преимущества в знании ключей сеанса. Ключи сессии, которые также основаны на случайных вкладах двух сторон, которые остаются неизвестными для атакующего злоумышленника.

– компрометация промежуточного ключа PMK (атака Деннинга-Сакко) не представляет преимущества для злоумышленника в определении другого ключа шифрования для другого выполнения протокола.

Помимо стандартного режима есть еще и переходный режим. Когда устройства, работающие как в WPA2-PSK, так и в WPA3-SAE, присутствуют в базовом наборе услуг (BSS) (рисунок 2.6), в этом случае точка доступа должна работать в режиме перехода WPA3-SAE.

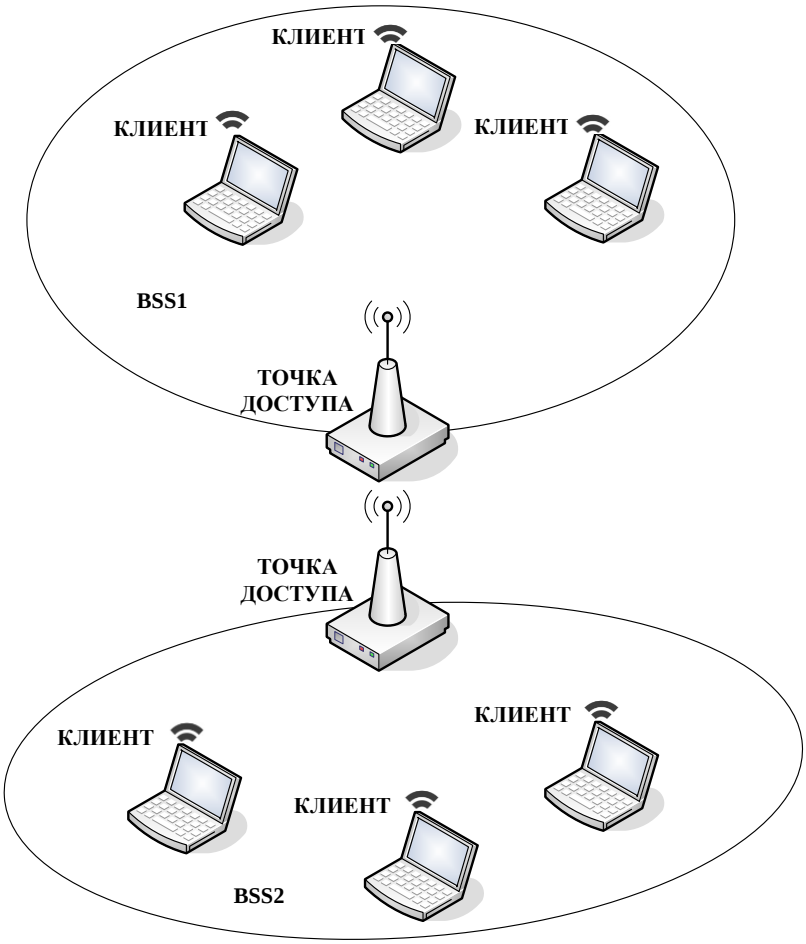

Рисунок 2.6 – Переходный режим WPA3-SAE

Таким образом, он может гарантировать доступ WLAN к обоим типам устройств, используя один и тот же пароль. Переходный режим будет в полной мере пользоваться всеми преимуществами, обеспечиваемыми использованием WPA3, поскольку некоторые функции должны быть принесены в жертву для обеспечения функциональной совместимости и совместимости двух систем. Очевидно, что этот режим предназначен только для временного использования WLAN, и здесь необходимо как можно скорее переключиться в режим, полностью совместимый с WPA3.

2.3.2 Реализация процедуры шифрования WPA3-Enterprise

В сетях, где безопасность является критическим фактором, предоставляется 192-битный режим безопасности, при этом он не является обязательным [7]. Для обеспечения согласованности этот режим обеспечивает минимальный уровень безопасности для криптографических примитивов всех элементов сети. 192-битный режим WPA3-Enterprise обеспечивает:

– использование 256-битного протокола режима Галуа/Счетчика (GCMP-256) для аутентификации и шифрования,

– использование 384-битного режима аутентификации хешированных сообщений (HMAC) с алгоритмом безопасного хеширования (HMAC-SHA384) для управления и проверки ключа,

– использование алгоритмов цифровой подписи эллиптической кривой (ECDH) и алгоритма цифровой подписи эллиптической кривой (ECDSA) для обмена ключами и аутентификации.

Чтобы использовать WPA3 enterprise, серверы (например RADIUS) должны использовать один из разрешенных шифров EAP:

– TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,

– TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384,

– TLS_DHE_RSA_WITH_AES_256_GCM_SHA384.

Чтобы использовать эту аутентификацию, сервер RADIUS должен поддерживать эти шифры. Кроме того, 192-битная защита WPA3 будет исключительной для EAP-TLS, для которого потребуются сертификаты как на сервере STA, так и на сервере RADIUS.

WPA3 - Enterprise следует тому же процессу, что и в WPA2, однако он улучшен благодаря вышеупомянутым шифрам.

Процесс WPA3 - Enterprise заключается в следующем (Рисунок 2.7):

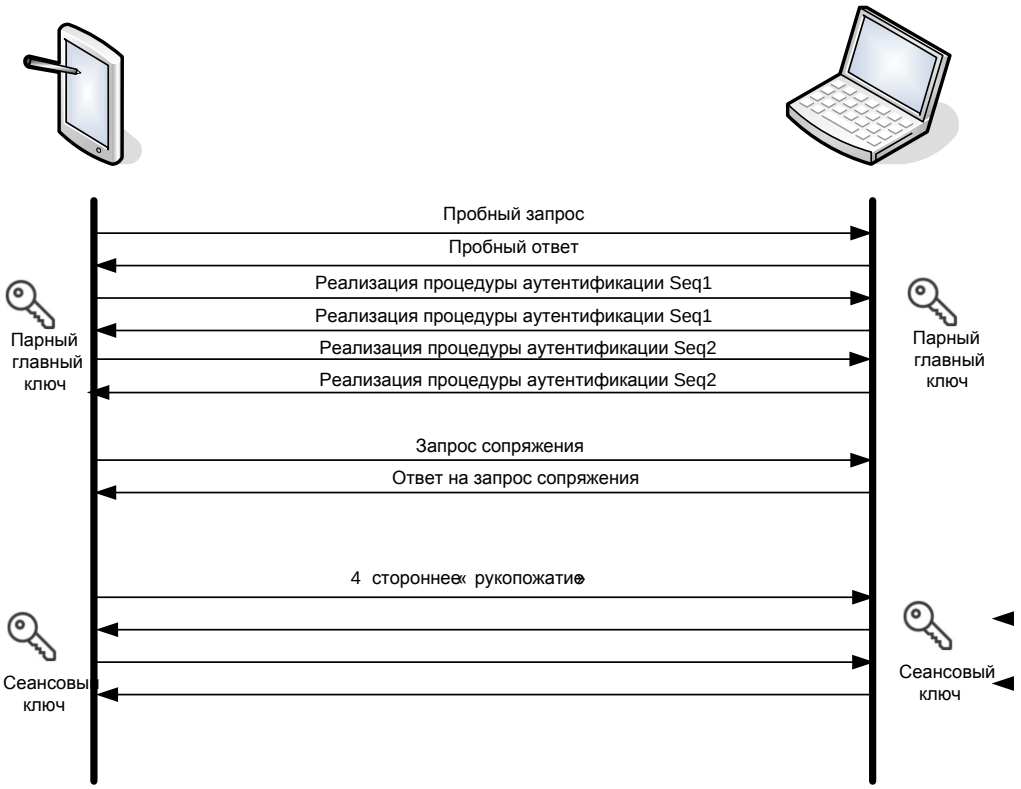

Рисунок 2.7 – Процесс шифрования WPA3 – Enterprise между двумя элементами сети

1. Пробный запрос:

– регулярный запрос к AP после маяка.

2. Пробный ответ:

– регулярный ответ на STA.

3. Аутентификация (фиксация) от STA к AP:

– этот пакет является аутентификацией 802.11,

– фиксация будет включать в себя аутентификацию SAE Seq1 между элементами, не связанную с используемым паролем.

– используется для генерации PMK (парного главного ключа) на STA.

4. Аутентификация (фиксация) от AP до STA.

– этот пакет является аутентификацией 802.11,

– фиксация будет включать в себя аутентификацию SAE Seq1 между элементами, не связанную с используемым паролем,

– используется для генерации PMK (парный главный ключ) на AP.

5. Аутентификация (подтверждение) от STA к AP.

– пакет является аутентификацией 802.11,

– подтверждение включает Seq2 с сообщением подтверждения с ключом, сгенерированным для AP, чтобы подтвердить.

6. Аутентификация (подтверждение) от AP до STA.

– пакет является аутентификацией 802.11,

– подтверждение включает в себя Seq2 с сообщением подтверждения с сгенерированным ключом, сообщающим STA, что ключ правильный или отклоняет аутентификацию.

7. Регулярный запрос на сопряжение (ассоциацию).

8. Регулярный ответ на сопряжение (ассоциацию).

9. Четырехстороннее взаимодействие с использованием PMK, созданного методом SAE. После этого шага обычные данные могут быть переданы.

Таким образом, каждый аспект управления ключами будет использовать достаточно надежную систему шифрования. Каждый клиент в сети должен работать в 192-битном режиме, под угрозой исключения из него и для WPA3-Enterprise нет необходимости в каком-либо переходном режиме.

2.3.3 Технология протокола Easy Connect

Ввод протокола Easy Connect в стандарт IEEE 802.11ax – это признание наличия в мире огромного количества устройств, присоединённых к сети [7]. И хотя, возможно, не все люди захотят обзавестись умными домами, у обычного пользователя к домашнему маршрутизатору сегодня, скорее всего, подключено больше устройств, чем в 2004 году. Easy Connect – попытка Wi-Fi альянса сделать подсоединение всех этих устройств более интуитивным. Вместо того чтобы каждый раз при добавлении устройства вводить пароль, у устройств будут уникальные QR-коды – и каждый код устройства будет

работать как публичный ключ. Для добавления устройства можно будет просканировать код при помощи смартфона, уже соединённого с сетью (Рисунок 2.8).

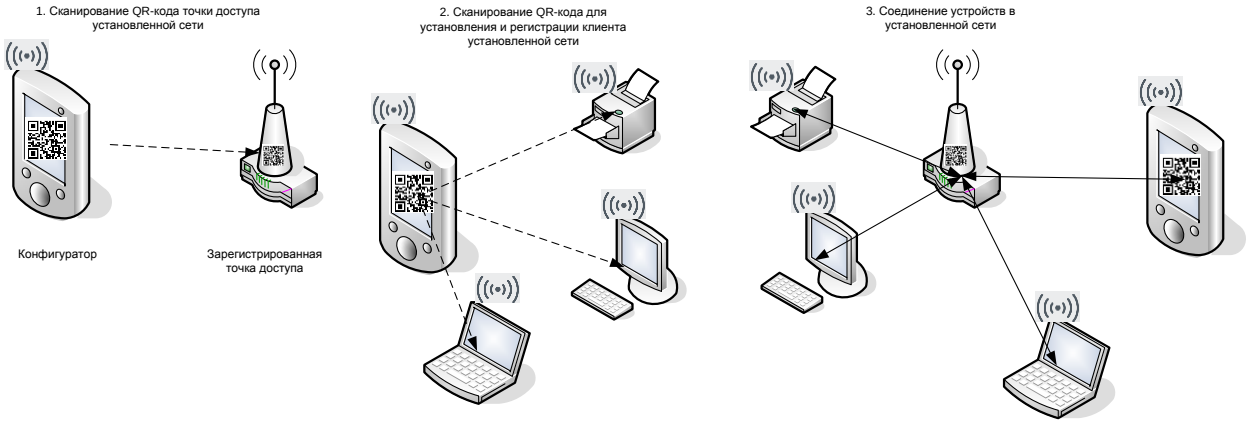

Рисунок 2.8 – Реализация соединения по протоколу Easy Connect

После сканирования устройство обменяется с сетью ключами аутентификации для установления последующей связи. Протокол Easy Connect не связан с WPA3 – устройства, сертифицированные для него, должны иметь сертификат для WPA2, но не обязательно сертификат для WPA3.

2.3.4 Реализация механизмов защиты по протоколу Enhanced Open

Enhanced Open [8] это ещё один отдельный протокол, разработанный для защиты пользователя в открытой сети. Открытые сети – такие, которыми пользуются в кафе или аэропортах несут в себе целый комплекс проблем, которые отсутствуют при работе в домашней сети.

Многие атаки, происходящие в открытой сети, относятся к пассивным. Когда к сети подключается большое количество пользователей, атакующий может собрать очень много данных, просто фильтруя проходящую информацию.

Enhanced Open использует «оппортунистическое» беспроводное шифрование (Opportunistic Wireless Encryption, OWE), определённое в

стандарте Internet Engineering Task Force RFC 8110, чтобы защищаться от пассивного подслушивания [8]. Для OWE не требуется дополнительная защита с аутентификацией – оно концентрируется на улучшении шифрования данных, передаваемых по публичным сетям, с целью предотвратить их кражу. Оно также предотвращает так называемую простую инъекцию пакетов (unsophisticated packet injection), в которой атакующий пытается нарушить работу сети, создавая и передавая особые пакеты данных, выглядящие, как часть обычного режима работы сети.

Процедура базового обмена кадрами в беспроводной сети по протоколу Enhanced Open представлена на рисунке 2.9.

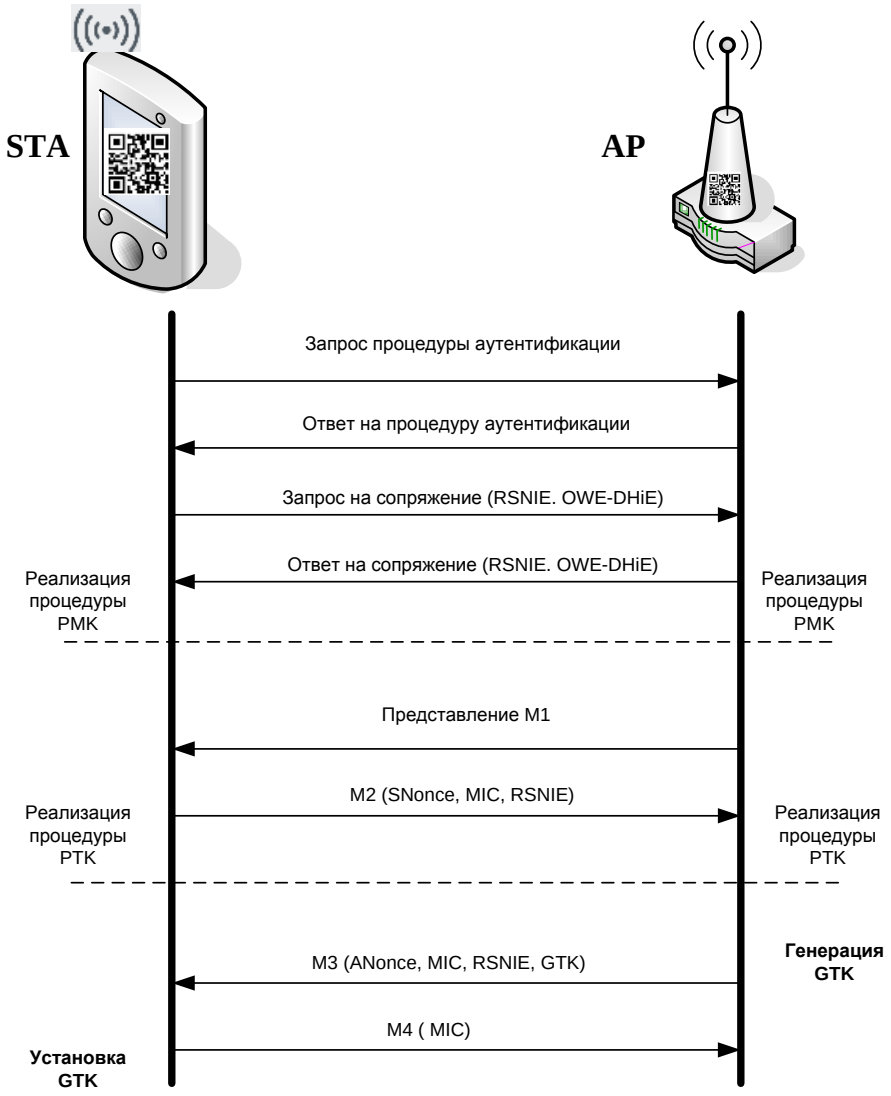

Рисунок 2.9 – Базовый обмен кадрами по протоколу Enhanced Open

Точка доступа (AP) объявляет о поддержке OWE с использованием селектора AKM suite для OWE в RSNE. Далее точка доступа сообщает о возможностях защиты кадра управления (MFP) и требуемом бите MFP и то же самое реализуется в кадре запроса ассоциации при отправке клиентом. Клиент, желающий сделать OWE, должен указать OWE AKM в части RSNE кадра запроса ассоциации и включить элемент параметра Диффи-Хелмана (DH). Кадр запроса сопряжения будет включать информационные элементы параметров RSNE & OWE-DH. Чтобы реализация была совместимой, она должна поддерживать DH-Group, которая представляет собой 256-битную эллиптическую кривую (ECP). Если AP не поддерживает группу DH, указанную в запросе на сопряжение, AP отвечает кодом состояния, указывающим неподдерживаемую группу. AP, согласная сделать OWE, должна включить OWE AKM в RSNE кадра ответа сопряжения. Если «кэширование PMK» не выполняется, оно также должно включать элемент параметра DH. Как только клиент завершит сопряжение, и клиент, и AP обмениваются своим ключом DH в этих кадрах запроса и ответа сопряжения. С этим STA & AP могут получить PMK (парный главный ключ), используя свой закрытый ключ, информацию об открытом ключе партнера и группу DH. PMKID генерируется путем хеширования двух открытых ключей DH и усечения до 128 бит. Алгоритм хеширования может быть «HMAC-SHA-256», «HMAC-SHA-384» или даже «HMAC-SHA-512». После завершения соединения 802.11 AP инициирует формальное четырехстороннее рукопожатие для получения ключей шифрования (KEK- Key Encryption Key ,KCK - Ключ подтверждения ключа и MIC - Код целостности сообщения).

Кэширование PMK поддерживается на SSID с расширенным открытием, где STA и AP могут кэшировать PMK в течение определенного периода времени. Как только клиент впервые подключается к OWE SSID, необходимо рассчитать значение PMKID.
Когда STA впоследствии подключается к той же AP, она может включать PMKID в кадр запроса сопряжения. Если AP кэшировала PMK,

идентифицированный этим PMKID, она включает этот PMKID в свой кадр ответа сопряжения. В этом случае не будет элемента параметра DH, включенного в этот кадр ответа ассоциации.

Enhanced Open не даёт защиты с аутентификацией из-за особенностей организации открытых сетей – они по определению предназначены для всеобщего использования. Enhanced Open был разработан для улучшения защиты открытых сетей против пассивных атак, так, чтобы не требовать от пользователей ввода дополнительных паролей или прохождения дополнительных шагов.

2.4 Выводы по разделу

1. Причиной эволюции стандарта Wi-Fi в IEEE 802.11ax стал такой важный тренд как «интернет вещей» (IoT). Исключительно важной является проблема безопасного и простого подключения сотен или более электронных устройств к корпоративной информационной системе в соответствии с их эксплуатационными, инженерными и технологическими потребностями.

2. В ходе эволюции стандартов сетей Wi-Fi скорость передачи данных увеличивалась за счет использования частотных ресурсов. В стандарте 802.11ax сам же выделенный спектр уже применяется более эффективно. И это позволяют реализовать следующие технологии:

- OFDMA,
- Resource Units,
- Target Wait Time (TWT),
- BSS coloring.

4. Появление встроенного в стандарт IEEE 802.11ax протокола беспроводной безопасности следующего поколения WPA3 является важным, поскольку он не только обеспечивает безопасность соединений Wi-Fi, но и помогает избавиться от корпоративных уязвимостей в области информационной безопасности.

5. Важнейшее изменение, которое принесёт WPA3 - это новый метод аутентификации устройств в сети. SAE (Simultaneous Authentication of Equals) – новый метод аутентификации устройства, пытающегося подключиться к сети. SAE – это вариант так называемого установления связи по методу «стрекозы», использующего криптографию для предотвращения угадывания пароля злоумышленником. Он говорит о том, как именно новое устройство, или пользователь, должен «приветствовать» сетевой маршрутизатор при обмене криптографическими ключами

6. Протокол SAE - это вариант Dragonfly, который предусматривает обмен ключами на основе доказательства с нулевым разглашением, поэтому пароль фактически не обменивается. С точки зрения безопасности, SAE - это протокол, который противостоит как пассивным, так и активным атакам, атакам по словарю и повторным атакам.

7. В сетях, где безопасность является критическим фактором, предоставляется 192-битный режим безопасности, при этом он не является обязательным. Для обеспечения согласованности этот режим обеспечивает минимальный уровень безопасности для криптографических примитивов всех элементов сети. Чтобы использовать WPA3 Enterprise, серверы (например RADIUS) должны использовать один из разрешенных шифров EAP. Каждый аспект управления ключами будет использовать достаточно надежную систему шифрования. Каждый клиент в сети должен работать в 192-битном режиме, под угрозой исключения из нее и для WPA3-Enterprise нет необходимости в каком-либо переходном режиме.

8. Ввод протокола Easy Connect в стандарт IEEE 802.11ax – это признание наличия в мире огромного количества устройств, присоединённых к сети. Easy Connect – попытка Wi-Fi альянса сделать подсоединение всех этих устройств более интуитивным. Вместо того чтобы каждый раз при добавлении устройства вводить пароль у устройств будут уникальные QR-коды и каждый код устройства будет работать как публичный ключ.

9. Enhanced Open это ещё один отдельный протокол, разработанный для защиты пользователя в открытой сети. Многие атаки, происходящие в открытой сети, относятся к пассивным. Когда к сети подключается большое количество пользователей, атакующий может собрать очень много данных, просто фильтруя проходящую информацию. Enhanced Open использует «оппортунистическое» беспроводное шифрование но не даёт защиты с аутентификацией из-за особенностей организации открытых сетей – они по определению предназначены для всеобщего использования. Enhanced Open был разработан для улучшения защиты открытых сетей против пассивных атак, так, чтобы не требовать от пользователей ввода дополнительных паролей или прохождения дополнительных шагов.

10. Некоторые общие, но фундаментальные факторы могут ослабить безопасность корпоративных сетей реализованных на базе стандарта IEEE 802.11ax такие как: не правильная конфигурация; плохие дизайнерские решения; устаревшее оборудование; устаревшее программное обеспечение. Все это требует совершенствования системы администрирования и контроля беспроводных сетей этого стандарта.

3 Разработка рекомендаций по защите корпоративной сети стандарта IEEE 802.11ax

3.1 Характеристика режимов функционирования беспроводной сети стандарта IEEE 802.11ax

Используя стандарт IEEE 802.11ax для работы корпоративной сети, предприятия могут ускорить внедрение так называемой интеллектуальной среды (Intelligent Edge) - места, где деловые действия, технологии и аналитика встречаются в режиме реального времени [7]. Благодаря встроенным в стандарт протоколам улучшается взаимодействие с конечными пользователями и приложениями, оптимизируются подключения для устройств IoT, а также обеспечивается автоматизация и контроль информационных технологий в реальном времени.

Возможно функционирование беспроводной сети стандарта в нескольких режимах, что помогает решить проблемы, которые могут возникнуть у предприятия сегодня, и позволяет подготовиться к тому, что будет завтра. Каждый из режимов требует специфического администрирования в интересах обеспечения информационной безопасности.

3.1.1 Режим безопасности приложений

Поскольку видео и голос являются наиболее важными ресурсами для телекоммуникационной компании беспроводные ресурсы становятся все более ценными.

В местах с высокой плотностью пользователей можно подключить сотни или даже тысячи одновременно работающих устройств в любой момент времени. Хотя каждая точка доступа может подключать десятки или даже сотни клиентских устройств, большой объем трафика, генерируемый

всего лишь частью устройств может привести к широкомасштабной производительности сети и как следствие задержке.

Решение этой задачи реализуется посредством оптимизации ресурсов. С помощью OFDMA, MU-MIMO и встроенного планирования ресурсов плотность устройств может быть увеличена до тысяч, а перегрузка сети в беспроводной локальной сети (WLAN) может быть значительно уменьшена. Это обеспечивает одновременное подключение большого количества пользователей в реальном времени, сверхнизкую задержку для AR/VR, видео и голоса 4K и многое другое. Эти возможности также могут улучшить существующие конфигурации QoS в сети, чтобы обеспечить гарантию приложений на уровне SLA (соглашение об уровне обслуживания).

3.1.2 Режим корпоративного охвата беспроводной сети

В организациях с распределенной инфраструктурой возникает потребность всеобъемлющего охвата структур организации для обеспечения постоянной связи, которая позволит партнерам и поставщикам услуг работать более тесно вместе. Данный режим позволяет решить проблему нестабильности внутреннего сотового покрытия.

Очень часто здания и сооружения ослабляют сотовые сигналы, особенно когда конечные пользователи перемещаются между этажами или в помещениях организации.

Используя Wi-Fi CERTIFIED 6 в сочетании с Wi-Fi CERTIFIED Passpoint, точки доступа WLAN, которые были оптимально развернуты внутри зданий, могут использоваться в качестве сети радиодоступа (RAN) для сотовая базовая сеть 5G. Это означает, что телефон сотрудника или гостя будет беспрепятственно подключаться к сети Wi-Fi с поддержкой Passpoint, входя в здание, если он находится на активном телефонном звонке или вводит текст СМС сообщения.

Это помогает предприятиям исключить преимущества развертывания оборудования для небольших ячеек, DAS или CBRS, а также обеспечивает доступ к указанным сетевым ресурсам.

3.1.3 Режим интеллектуальной области

Поскольку при глубокой интеграции в компаниях бизнес-транзакции становятся гиперсвязанными возникает потребность в обеспечении взаимной цифровой трансформации. Многие приложения и данные, которые были перенесены в централизованные облака, порождают растущий объем информации с увеличением числа подключенных устройств, что приводит к увеличению задержки в сети, снижению производительности и росту затрат, а имеющаяся в организации инфраструктура не может вместить такой ресурс.

Использование Wi-Fi 6 в этом случае может решить задачу интеграции автоматизированных рабочих мест в интересах решения ключевых технологических задач. В этом случае компании и организации могут использовать Wi-Fi 6 в качестве средства, позволяющего получать информацию о предприятиях и реагировать на них в режиме реального времени, обеспечивая более высокую производительность, емкость и сверхнизкую задержку. По мере появления новых сценариев использования, таких как пограничные вычисления, 5G и IoT, Wi-Fi 6 упрощает процедуры подключение людей и оборудования на периферии, приложений и данных в облаке, а также позволяет осуществлять контроль и решать локальные задачи.

3.1.4 Режим центра конвергенции «интернет вещей»

По мере расширения использования технологий IoT WLAN становятся естественным центром конвергенции. В условиях активного развития IoT возникает проблема комплексного управления технологическими

процессами. Информационным отделам в этом случае необходимо поддерживать независимые системы или сетевые приложения для обеспечения возможности подключения устройств (например, камер наблюдения и датчиков), что делает управление громоздким и неэффективным.

В этом случае Wi-Fi 6 может быть применена в режиме поддержки нескольких беспроводных подключений. В качестве основного метода подключения для мобильных пользователей и появляющегося набора клиентских устройств в этом случае возможно использование WLAN для подключения сотен или даже тысяч устройств Wi-Fi 6 к одной точке доступа. Кроме этого поддерживается возможность использования беспроводных носителей, таких как Bluetooth, Zigbee и другого оборудования. Это позволяет предприятиям объединять беспроводные технологии на единой платформе и улучшить взаимодействие и контроль, чтобы сократить расходы и оптимизировать ресурсы.

3.1.5 Режим информационной безопасности

Физическая и информационная безопасность остаются приоритетными в любой организации и компании. Wi-Fi 6 может занять в их обеспечении ключевую роль.

С учетом специфики предприятий гостевой трафик может передаваться в открытом виде. Чаще всего конечные пользователи, которые подключаются к общедоступному Wi-Fi подключаются к открытой WLAN без символа блокировки в раскрывающемся меню. Это означает, что любой злоумышленник может потенциально выполнить захват пакета личной информации и получить доступ к финансовым учетным записям или другой конфиденциальной информации. До сих пор рекомендации по борьбе с этой ситуацией включали использование VPN или же исключение подключения вообще.

Применение Wi-Fi 6 может реализовать шифрование сетей с использованием Wi-Fi CERTIFIED WPA3 и Wi-Fi CERTIFIED Enhanced Open. Спустя почти два десятилетия с момента появления Wi-Fi CERTIFIED WPA2 и открытых сетей предприятия теперь могут развертывать WPA3 и Wi-Fi Enhanced Open для реализации процедур шифровки сетевого трафика сотрудников и гостей без нарушения работы пользователей. Гости могут продолжать подключаться к «открытой» сети, и при этом будет обеспечиваться безопасный Wi-Fi с собственным шифрованием.

3.2 Рекомендации по конфигурированию беспроводной сети стандарта IEEE 802.11ax

Wi-Fi стал важным средством подключения для обеспечения мобильности и создания условий для совместной работы. Первый этап создания условий реализует задачу оптимальной конфигурации оборудования и программного обеспечения сети [7].

Шаг 1 предусматривает размещение маршрутизатора Wi-Fi для оптимального покрытия сети (рисунок 3.1).

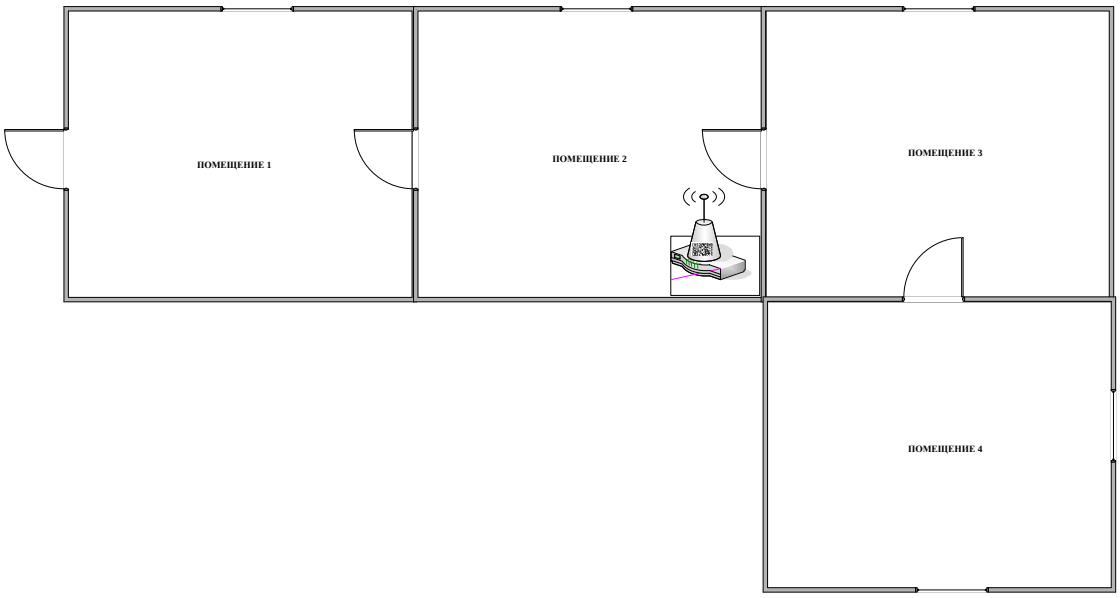

Рисунок 3.1 – Размещение маршрутизатора в компании

Размещение маршрутизатора является ключом к обеспечению надежного, высококачественного покрытия Wi-Fi всей компании. Вместо того, чтобы размещать маршрутизатор в удаленном углу, где стены или другие препятствия могут снизить производительность, необходимо найти центральное место, чтобы максимально увеличить зону покрытия устройства и обеспечения надежного сигнала Wi-Fi по всем помещениям компании.

Шаг 2 предусматривает обновление оборудования корпоративной Wi-Fi. Важно, чтобы сетевое оборудование Wi-Fi в компании было обновлено в соответствии с требованиями растущего числа и типов устройств. Последняя версия Wi-Fi - Wi-Fi 6 - уже внедряется в такие продукты, как точки доступа и смартфоны. В этом случае Wi-Fi 6 обеспечивает максимальную емкость, эффективность и покрытие, необходимые для продуктивной работы в организации.

Шаг 3 предусматривает исключение из работы информационной системы не сертифицированного оборудования. Сертифицированное Wi-Fi оборудование важно для обеспечения того, чтобы все устройства компании обеспечивали защиту Wi-Fi и работали с другими корпоративными устройствами. Сертифицированные устройства Wi-Fi проходят строгие испытания для обеспечения их соответствия отраслевым стандартам. Сертифицированные устройства Wi-Fi обеспечивают максимально надежную и стабильную работу Wi-Fi даже при использовании высокопроизводительных приложений. Важно наличие на этом оборудовании логотипа Wi-Fi Certified.

Шаг 4 предполагает проверку настроек безопасности сети Wi-Fi.

Выбор устройств Wi-Fi Certified обеспечивает гарантии того, что устройства Wi-Fi включают новейшие средства защиты, описанные во втором разделе. Последняя версия безопасности Wi-Fi, WPA3 потребуется во всех сертифицированных устройствах и предоставляет на рынок самые современные протоколы безопасности. Многие устройства уже поддерживают новейшую защиту, но во время перехода на WPA3

пользователи по-прежнему остаются защищенными путем выбора надежного пароля и включения шифрования.

Шаг 5 требует использования Wi-Fi звонков. Особенно это важно если имеют место проблемы с сотовой связью в этом случае звонки по Wi-Fi - это опция, которая позволит выполнять голосовые звонки с мобильного устройства с Wi-Fi. Вызов Wi-Fi позволяет совершать вызовы через сеть Wi-Fi. При правильной настройке процесс является практически бесперебойным, и нет разницы в качестве. При этом нет необходимости подписываться на специальный тарифный план или покупать новое оборудование, просто включается вызов Wi-Fi через интерфейс на мобильном устройстве.

Все эти конфигурационные рекомендации можно объединить в общую системную последовательность (Рисунок 3.2.)

Рисунок 3.2 – Конфигурационные рекомендации по организации беспроводной сети IEEE802.11ax

3.3 Рекомендации по администрированию сети IEEE 802.11ax

Анализ защищенности Wi-Fi сети может основываться на тщательном анализе возможных действий злоумышленников, направленных на реализацию различных угроз нарушения безопасности. Используя уязвимости и недостатки в конфигурации беспроводной сети злоумышленники реализуют разнообразные стратегии нападения. Эти стратегии могут быть направлены как на различные критические важные информационные ресурсы сети, так и на деструктивные действия связанные с процессом функционирования сети.

Высокая сложность Wi-Fi сети стандарта IEEE 802.11ax и новизна механизмов защиты существенно затрудняют возможности по реализации атак злоумышленниками. Поэтому администраторам информационных систем, где имеют место сегменты беспроводных сетей, необходимо регламентировать действия их организационному, техническому и программному сопровождению. Алгоритмы такого сопровождения целесообразно включить в регламент функционирования беспроводной сети и в целом в политику обеспечения информационной безопасности.

Классические атаки, такие как дешифрование [23] трафика и внедрение [24] пакетов, больше не возможны, поскольку они эффективно смягчаются с помощью PFS и введением AES в WPA2. Существует атака на сети Wi-Fi под названием Evil Twin Attack [25], которая требует некоторого взаимодействия с пользователем, но все равно будет работать с WPA3.

Теория этого проста: все, что злоумышленнику необходимо знать для клонирования AP, это SSID, схема аутентификации и маркер аутентификации - в данном случае PSK. Знание PSK является самым большим препятствием для проведения этой атаки. Успешная атака Evil Twin переводит злоумышленника в положение «Человек посередине» (MiTM) без необходимости что-либо эксплуатировать, поскольку пользователь уже подключен к сети. Как только позиция MiTM была получена, можно

перехватывать и изменять незашифрованный трафик, такой как HTTP, FTP и другие незашифрованные протоколы. К сожалению, на настоящий момент нет никаких технических мер по уходу от этой проблемы.

В следующей таблице 3.1 приведен краткий обзор некоторых известных атак на персональные сети и того, какой стандарт уязвим:

Таблица 3.1 - Обзор известных атак на персональные сети по протоколам безопасности

Attack	WPA2-TKIP	WPA2-PSK-CCMP	WPA3-PSK-CCMP
Clientless Password Cracking			
Cracking four-way handshake			
Downgrade Attacks			
Timing-based side-channel			
Cache-based side-channel			
Decrypting sniffed Traffic (with PSK)			
Evil Twin (with PSK)			
KRACK Attack			
Injecting Traffic			
Deauthentication			
Hole 196			

color	connotation
Vulnerable	
Implementation dependant	
Not Vulnerable	
Not Applicapable	

Анализ таблицы показывает, что уровень защиты беспроводных сетей стандарта IEEE 802.11ax со встроенным протоколом безопасности WAP3 значительно выше, чем использованные ранее WAP2 и их модификации и при администрировании требует четкой регламентации действий. На основе анализа механизмов защиты, встроенных в стандарт IEEE 802.11ax можно сформировать типовой алгоритм действий администратора информационной системы и выделить в нем наиболее значимые действия, реализуемые при контроле службой информационной безопасности (Рисунок 3.3)

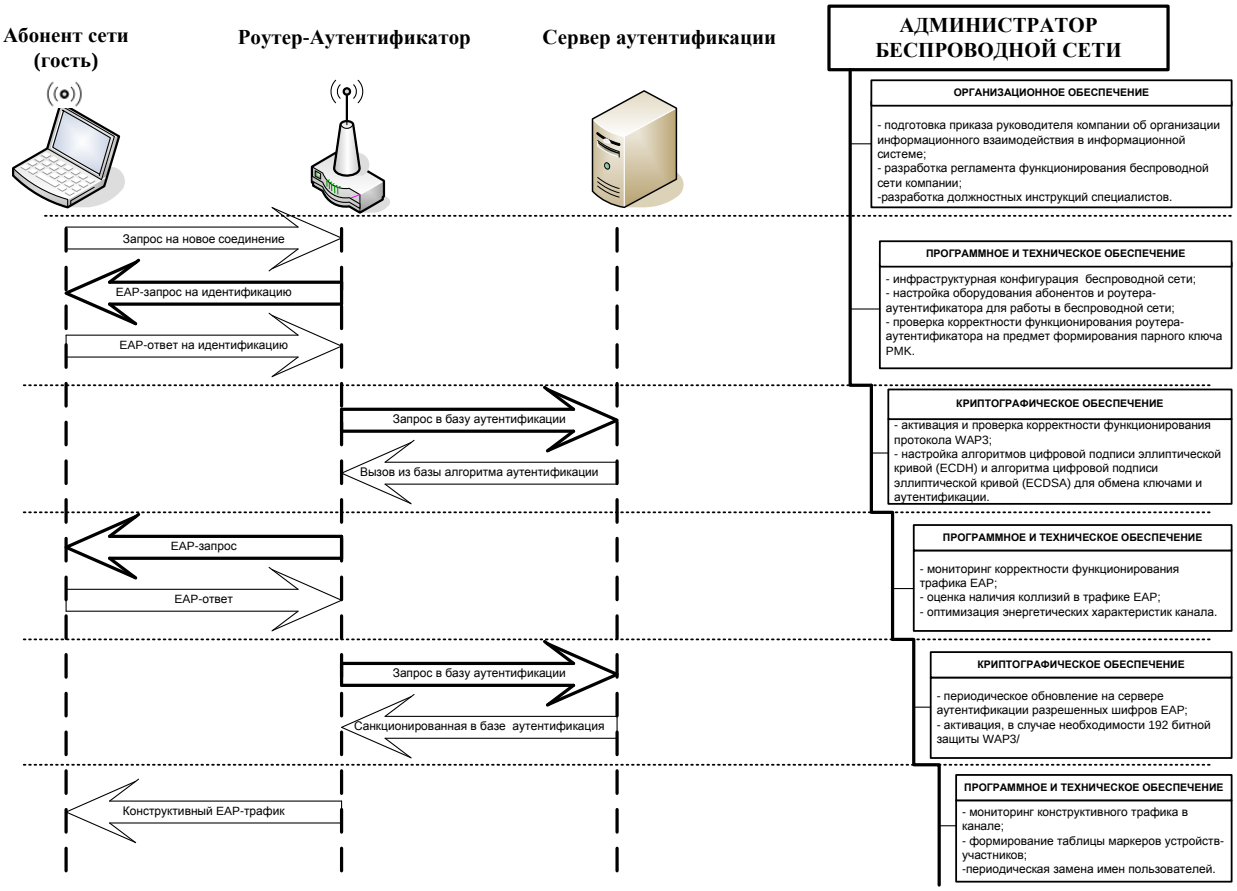

Рисунок 3.3 – Алгоритм действий при администрировании беспроводной сети стандарта IEEE 802.11ax

Анализируя процесс администрирования и проецируя его в область аудита Wi-Fi сети, возможно выделение комплекса задач требующих периодического или постоянного решения:

– проведение анализа конфигурации сети,

– мониторинг процессов, происходящих в сети,

– моделирование действий злоумышленников на основе данных о сети,

– построение цепочки возможных атакующих действий, выполняемых из различных точек беспроводной сети и направленных на реализацию различных угроз информационной безопасности,

– определение уязвимостей и узких мест в защите беспроводной сети,

– оценка показателей защищенности и определение общего уровня защищенности беспроводной сети,

– выработка рекомендаций по усилению защищенности в целом информационной системы.

3.4 Выводы по разделу

1. В разделе проведена разработка рекомендаций по защите корпоративной Wi-Fi сети стандарта IEEE 802.11ax. Отмечено, что функционирование беспроводной сети стандарта может осуществляться в нескольких режимах, что помогает решить проблемы, которые могут возникнуть у предприятия сегодня, и позволяет подготовиться к тому, что будет завтра. Выделено 5 режимов:

- режим безопасности приложений, который реализуется посредством оптимизации ресурсов,

- режим корпоративного охвата беспроводной сети который позволяет решить проблему нестабильности внутреннего сотового покрытия,

- режим интеллектуальной области - использование Wi-Fi 6 в этом случае может решить задачу интеграции автоматизированных рабочих мест в интересах решения ключевых технологических задач,

- режим центра конвергенции – решается задача комплексного управления технологическими процессами,

- режим центра конвергенции «интернет вещей».

2. Физическая и информационная безопасность остаются приоритетными в любой организации и компании. Wi-Fi 6 может занять в их обеспечении ключевую роль.

3 Важным является конфигурирование беспроводной сети стандарта IEEE 802.11ax, которое реализуется на основе пяти основных шагов:

- шаг 1 предусматривает размещение маршрутизатора Wi-Fi для оптимального покрытия сети,

- шаг 2 предусматривает обновление оборудования корпоративной Wi-Fi и здесь важно, чтобы сетевое оборудование Wi-Fi было обновлено в соответствии с требованиями растущего числа и типов устройств,

- шаг 3 предусматривает исключение из работы информационной системы не сертифицированного оборудования,

- шаг 4 предполагает проверку настроек безопасности сети,

- шаг 5 требует использования Wi-Fi звонков, особенно это важно, если имеют место проблемы с сотовой связью в этом случае звонки по Wi-Fi - это опция, которая позволит выполнять голосовые звонки с мобильного устройства с Wi-Fi.

Все эти конфигурационные рекомендации можно объединить в общую системную последовательность.

4. Высокая сложность Wi-Fi сети стандарта IEEE 802.11ax и новизна механизмов защиты существенно затрудняют возможности по реализации атак злоумышленниками. Поэтому администраторам информационных систем, где имеют место сегменты таких беспроводных сетей, необходимо регламентировать действия их организационному, техническому и программному сопровождению.

5. Проведен обзор известных атак на персональные сети по протоколам безопасности, данные сведены в таблицу. Анализ таблицы показывает, что уровень защиты беспроводных сетей стандарта IEEE 802.11ax со встроенным протоколом безопасности WAP3 значительно выше, чем использованные ранее WAP2 и их модификации и при администрировании требует четкой регламентации действий.

6. На основе анализа механизмов защиты, встроенных в стандарт IEEE 802.11ax сформирован алгоритм действий администратора информационной системы, который привязан к основным процессам функционирования сети. В алгоритме выделены наиболее значимые действия, реализуемые при контроле службой информационной безопасности.

7. Анализируя процесс администрирования и проецируя его в область аудита Wi-Fi сети, возможно выделение комплекса задач требующих периодического или постоянного решения:

- проведение анализа конфигурации сети,
- мониторинг процессов, происходящих в сети,
- моделирование действий злоумышленников на основе данных о сети,
- построение цепочки возможных атакующих действий, выполняемых из различных точек беспроводной сети и направленных на реализацию различных угроз информационной безопасности,
- определение уязвимостей и узких мест в защите беспроводной сети,
- оценка показателей защищенности и определение общего уровня защищенности беспроводной сети,
- выработка рекомендаций по усилению защищенности в целом информационной системы.

4 Технико-экономическое обоснование предлагаемых мер по защите информации в беспроводной сети стандарта IEEE 802.11ax

4.1 Подходы к обоснованию затрат на информационную безопасность

В обосновании затрат на информационную безопасность (ИБ) существует два основных подхода [45]. Первый подход определяется экспертами как наукообразный, и заключается в том, чтобы освоить, а затем и применить на практике необходимый инструментарий измерения уровня ИБ. Для этого необходимо привлечь руководство компании, как ее собственника, к оценке стоимости информационных ресурсов, определению оценки потенциального ущерба от нарушений в области ИБ. От результатов этих оценок будет во многом зависеть дальнейшая деятельность ответственных специалистов в области ИБ. Если информация ничего не стоит, существенных угроз для информационных активов компании нет, а потенциальный ущерб минимален и стратегическое руководство компании это подтверждает, то проблема обеспечения ИБ является не актуальной. Если информация обладает определенной стоимостью, угрозы и потенциальный ущерб ясны, тогда актуализируется вопрос о внесении в бюджет расходов на подсистему ИБ. В этом случае в обязательном порядке необходима поддержка руководства компании в осознании проблем ИБ и построении системы защиты информации.

Второй подход эксперты в области ИБ определяют как практический, и состоит он в следующем: можно попытаться найти аналог разумной стоимости системы защиты информации. При этом существуют аналогичные инварианты в других областях, где значимые для компаний события носят вероятностный характер. Например, на рынке автострахования оценка стоимости этой успуги составпяет - 5-15% от рыночной стоимости автомобипя в зависимости от локальных условий его эксппуатации, стажа

водителя, интенсивности движения, состояния дорог и т.д [45].

По аналогии, ИБ в компании можно вообще не заниматься, и не исключен такой вариант, что принятый риск себя вполне оправдает. При этом можно потратить на создание системы защиты информации немало средств, и при этом может остаться некоторая уязвимость, которая рано или поздно приведет к утечке или хищению важной для компании информации.

Эксперты в обпасти ЗИ нашли оптимальное решение, при котором руководству компании можно чувствовать себя уверенно - стоимость системы ИБ должна составлять примерно 10-20% от стоимости ИС, в зависимости от конкретных требований к режиму ИБ. Это и есть та самая оценка на основе практического опыта, которой можно пользоваться, если не производить детальные расчеты.

Этот подход не лишен недостатков. Высока вероятность, что не удастся мотивировать руководство в острое осознание проблем ИБ. При этом можно обосновать объем бюджета на ИБ путем ссыпки на понятные большинству владельцев информационных ресурсов общепринятые требования к обеспечению режима информационной безопасности «best practice», формализованные, например, в стандарте ISO 17799.

Оценка затрат на практике существенно зависит от многих факторов, среди которых основными являются степень зрелости организации и специфика ее деятельности. Многие решения в области ЗИ часто принимаются на уровне интуиции, без каких-либо экономических расчетов и обоснований. В результате только те специалисты, которые за счет своей компетентности смогли заявить и отстоять потребность в ЗИ имеют возможность повлиять на планирование бюджета компании на ИБ. При этом современные требования ведения бизнеса определяют целесообразность применения в деятельности компаний современных и обоснованных технико-экономических методов и средств, позволяющих количественно измерять уровень защищенности компании, а также оценивать экономическую эффективность затрат на ИБ [45].

Учитывая, что практический результат совершенствования СУИБ в итоге предполагает корректировку Политики информационной безопасности компании, в части касающихся мероприятий по управлению, задача технико-экономического обоснования будет состоять в стоимостной оценке объекта интеллектуальной собственности (ОИС), которым по сути, является этот документ.

4.2 Оценка стоимости объектов интеллектуальной собственности

Оценка стоимости объектов ОИС, созданных в компании или по ее заказу с закреплением за ней по договору прав собственности на них, производится по затратному методу и определяется по формуле (1) [46]:

$$С=Ср+Сп+См, \quad (1)$$

где: Ср - приведенные затраты на создание ОИС, руб.,

Сп - приведенные затраты на правовую охрану ОИС, руб.,

См - приведенные затраты на маркетинговые исследования, руб.

Приведенные затраты на создание ОИС (Ср) – сумма фактически произведенных затрат на выполнение оценочных работ в полном объеме (от поиска материалов исследования до формирования отчета) и разработку всей последующей документации.

Приведенные затраты для оценочных работ состоят из затрат на поисковые работы, включая предварительную проработку проблемы, на теоретические исследования, на проведение экспериментов, испытаний, на услуги сторонних организаций, на составление, рассмотрение и утверждение отчета и прочих затрат.

Приведенные затраты на разработку технической документации (ТД) состоят из затрат на выполнение эскизного проекта, технического задания, рабочего проекта, расчетов, испытаний, услуг сторонних организаций,

авторского надзора, дизайна. Кроме того, сюда включаются затраты на доведение ОИС до готовности использования и реализации.

В тех случаях, когда документация выполняется частично или созданию ОИС предшествует проведение только оценочной работы или разработка технической документации, то расчет стоимости ОИС производится по затратам на фактически выполненные работы, что собственно и характерно для нашего случая.

Приведенные затраты на правовую охрану ОИС (Сп) – затраты на оформление заявочных материалов на получение патента (свидетельства), переписка по заявке, оплата пошлин за проведение экспертизы, получение патента (свидетельства) и поддержание его в силе и т.д.

Приведенные затраты на маркетинговые исследования (См). Для целей приведения разновременных стоимостных оценок к конечному году применяется коэффициент α_i , но в данном случае он будет равен 1, потому что число лет, предшествующих расчетному году равно 0.

Затраты, произведенные на выполнение оценочных работ и разработку всех стадий ТД, то есть Ср могут включать в себя [46]:

- израсходованные материальные ресурсы,

- оплата труда с отчислениями разработчиков,

- амортизационные отчисления оборудования, которое использовалось при разработке ОИС,

- аренда помещения для разработчиков.

Кроме того, создание любого ОИС или разработка программного обеспечения происходит не всегда согласно задания, где четко оговорены сроки работы. Разработчик может вне плановых заданий выполнить ОИС или написать программу для ПЭВМ. В случае если отсутствует документация по затратам на создание ОИС, то их можно определить расчетным путем. Затраты на создание ОИС на соответствующем временном отрезке t определяются по следующей формуле (2):

$$Cпр = \left(\frac{З}{m} \right) Kt, \qquad (2)$$

где: *З* - среднемесячная заработная плата разработчика (или команды разработчиков) с учетом районного коэффициента, руб.,

m - среднее количество рабочих часов в месяце, часов,

K - коэффициент, учитывающий отчисления с заработной платы (единый социальный налог и страховые взносы), *K*=1,30,

t - время, затрачиваемое разработчиком (командой разработчиков) на создание (разработку) ОИС, на отладку и адаптацию ОИС к условиям производства, дней.

Для расчета себестоимости потребуются затраты времени. Данный ОИС разрабатывался согласно заявке Генерального директора ООО «Медиа-техника» г. Ставрополь. При этом весь перечень произведённых работ не был определен рамками задания с указанием конкретных сроков выполнения. Были выделены только основные этапы разработки.

Для обеспечения наибольшей достоверности временных затрат используем метод экспертных оценок [46]. Экспертные исследования могут иметь как самостоятельное значение, так и использоваться при проверке истинности (верификации) логических исследований и моделирования. Прогнозные экспертные оценки отражают индивидуальность суждения специалистов относительно эффективности, расхода ресурсов, безопасности, а также перспектив развития объекта и основаны на мобилизации профессионального опыта и интуиции.

Время работы, по разработке рекомендаций по защите информации в беспроводной сети и как следствие корректировку разделов Политики ИБ, учтём в соответствующих этапах. Для определения средних значений a_{icp} m_{icp} и b_{icp} используются экспертные оценки, и данные специалистом, отвечающим за вопросы ИБ и автором выпускной квалификационной

работы. Средние значения найдём по формуле (3). Значения m_i и b_i рассчитываются аналогично.

$$a_{icp} = \frac{\left(3a_{ipry} + 2a_{iaав}\right)}{2}, \qquad (3)$$

где: a_{ipry} - оценка, данная руководителем,

$a_{iaав}$ - оценка, данная автором.

Затраты времени на разработку ОИС приведены в таблице 4.1.

Таблица 4.1- Затраты времени на разработку ОИС

Этапы разработки ОИС	Минимально возможная величина затрат, чел. час.			Наиболее вероятная величина затрат, чел. час.			Максимально возможная величина затрат, чел. час.		
	Руководитель	Автор	Средняя	Руководитель	Автор	Средняя	Руководитель	Автор	Средняя
Ознакомление с исходными данными	2	4	3	3	5	4	4	7	5,5
Написание введения	1	2	1,5	2	3	2,5	3	4	3,5
Проведение анализа информационных ресурсов компании	10	11	10,5	12	13	12,5	13	14	13,5
Анализ процессов функционирования беспроводной сети	12	13	12,5	14	16	15	16	20	18
Исследование социальной инженерии	90	92	91	94	96	95	96	98	97
Разработка рекомендаций по защите информации в беспроводной сети	110	110	110	120	155	137,5	130	160	145
Написание заключения и корректировка разделов политики ИБ	4	5	4,5	5	6	5,5	6	8	7
Всего	229	237	233	250	294	272	268	311	289,5

Ожидаемая величина затрат времени для *i*-го этапа (MO*i*) и стандартное отклонение этой величины каждого *i*-го этапа (G*i*) расчитываются как:

$$MO_i = \frac{a_i + 4m_i + b_i}{6}, \quad (4)$$

$$G_i = \frac{b_i - a_i}{6}, \quad (5)$$

где: a_i - наименьшая величина затрат времени для *i*-го этапа разработки;

m_i - наиболее вероятная величина затрат времени для *i*-го этапа;

b_i - наибольшая величина затрат времени для *i*-го этапа.

Результаты расчетов сводятся в таблицу 4.2.

Таблица 4.2- Затраты времени на разработку ОИС

Этапы разработки ОИС	Средняя величина затрат времени этапа разработки ОИС, чел.час.			Оценка затрат времени (MO*i*)	Стандартное отклонение (*Gi*)
	Минимально возможная (*ai*)	Наиболее вероятная (*mi*)	Максимально возможная (*bi*)		
Ознакомление с исходными данными	3	4	5.5	3,8	0,4
Написание введения	1,5	2,5	3,5	2,5	0,3
Проведение анализа информационных ресурсов компании	10,5	12,5	13,5	12,3	0,5
Анализ процессов функционирования беспроводной сети	12,5	15	18	15,1	0,9
Исследование социальной инженерии	91	95	97	94,6	1,0
Разработка рекомендаций по защите информации в беспроводной сети	110	137,5	145	134,1	5,8
Написание заключения и корректировка разделов политики ИБ	4,5	5,5	7	5,6	0,4

Зная ожидаемые затраты и стандартное отклонение по каждому этапу, рассчитываются эти показатели в целом по ОИС:

$$MO = \sum_{i=1}^{n} MO_i, \quad (6)$$

$$G = \sqrt{\sum_{i=1}^{n} G\,i^2} \quad (7)$$

Таким образом:

MO = 3.8 + 2,5 + 12,3 + 15,1 + 94,6 + 134,1 + 5,6 = 268;

$$G = \sqrt{0{,}4^2 + 0{,}3^2} + 0{,}5^2 + 0{,}9^2 + 1^2 + 5{,}8^2 + 0{,}4^2 = 6{,}01.$$

4.3 Расчет стоимости подготовленной документации

Возникает задача определения себестоимости разработки подготовленной документации, необходимой для оценки текущего уровня защищённости информации компании, выполнения требований законодательства РФ, документов и стандартов в области ИБ [45].

Стоимость разработки ОИС найдём по формуле (2) при следующих данных:

- среднемесячная заработная плата разработчика с учетом районного коэффициента составляет 25 000,00 руб.;
- среднее количество рабочих часов в месяце: 168 часов;
- затраты времени на разработку ОИС: 268 + 6=274 часа.

Итоговый результат будет иметь вид:

$$C = \left(\frac{25000}{168}\right) \cdot 1{,}3 \cdot 274 = 53005{,}95\,руб.$$

4.4 Расчет капитальных затрат

Капитальные затраты на приобретение и внедрение программного обеспечения определяются на контрактной или договорной основе заказчиком и подрядчиком [45]. Эта информация является

конфиденциальной, поэтому в расчётах использованы цены на ПО, размещённые поставщиками на информационных ресурсах в сети Интернет.

Капитальные затраты по данному проекту:

- затраты на разработку документации;
- затраты на закупку вычислительной техники;
- затраты на закупку лицензий программного обеспечения.

Затраты на приобретение системного ПО отсутствуют, так как проект реализуется на программных ресурсах компании, имеющей лицензии на операционную систему. В качестве вычислительной техники используется рабочий ноутбук администратора информационной системы. Средняя стоимость 4-х ядерного ноутбука с 8Гб оперативной памяти по ценам магазина цифровой и бытовой техники «Ситилинк» составляет 30 000 руб. Стоимость пакета Microsoft Office 2019 в магазине «DNS» составляет 15000 руб. Цены приведены на 8.05.2020 Величина капитальных затрат сведена в таблицу 4.3.

Таблица 4.3 – Капитальные затраты (вариант)

Наименование затрат	Детализация	Сумма, руб.
Затраты на разработку документации	Политика информационной безопасности (раздел – информационная система организации)	53005,95
Затраты на закупку вычислительной техники	Ноутбук 14" Ноутбук HP Chromebook x360 14b-ca0000ur	29999,00
Затраты на закупку лицензий программного обеспечения	Пакет Microsoft Office 2019	17999
Итого:		101003,95

4.5 Расчет эксплуатационных расходов

Эксплуатационные расходы — это текущие расходы предприятия на эксплуатацию.

Эксплуатационные расходы включают:

- амортизационные отчисления;
- затраты на электроэнергию;
- прочие расходы.

Амортизация — это процесс постепенного возмещения стоимости основных фондов, переносимой на вновь созданную продукцию, в целях накопления средств для реконструкции и приобретения основных средств [45]. Величина амортизационных отчислений определяется установленной долей ежегодных отчислений (норма амортизации) от стоимости основных средств и рассчитывается по формуле, представленной ниже (в рублях).

$$AO = Ф \cdot H_a \cdot K, \quad (8)$$

где: H_a - норма амортизации %,

$Ф$ - средняя годовая стоимость фондов (капитальные вложения),

K – *коэффициент* (K=0,41, что составляет 5 месяцев от 1 года).

Рассчитаем норму амортизации по формуле 9.

$$H_a = \frac{1}{n} \cdot 100 \quad (9)$$

где: n – срок эксплуатации, лет.

$$H_a = \frac{1}{4} \cdot 100 = 25\%;$$

В целом амортизационные расходы составят:

$$AO = 30000 \cdot 25 \cdot 0{,}41 = 3075 руб / год.$$

Определим затраты на электроэнергию. Электроэнергия, потребляемая для нужд компании, рассчитывается по видам оборудования, исходя из его мощности, продолжительности работы и действующему тарифу на электроэнергию. В данном проекте предусмотрен 1 ноутбук, с мощностью

0,44 кВт. Затраты на электроэнергию рассчитываются по формуле (10) в рублях:

$$З_{ээ} = N = Tt\sum P_{потр}N_i, \quad (10)$$

где: T – тариф за 1 кВт/час потребляемой электроэнергии в рублях,

t – продолжительность работы оборудования в год в часах,

$P_{потр}$ - потребляемая мощность в кВт,

N_i - количество i-го вида оборудования в единицах.

Среднюю продолжительность работы оборудования в компании найдём по формуле (11) в часах:

$$t = nm, \quad (11)$$

где: n-количество рабочих дней (n=397,1 часов=49,64 дней),

m - количество рабочих часов в день (учитывая особенности работы сервера службы каталогов, m=8 часов).

t = 49,64·8 = 397,1 часа и $З_{ээ}$= 4,55·397,1·0,44·1 = 794,99 руб.

Суммарные расходы за всё время реализации модели угроз приведены в таблице 4.4.

Таблица 4.4 - Суммарные расходы

Наименование затрат	Сумма затрат, руб.
Затраты на амортизацию	3 075,00
Затраты на электроэнергию	794,99
Прочие расходы (5% от капитальных затрат)	9679,88
Итого	13549,87

Итоговые расходы с учетом капитальных затрат:

101003,95 + 13549,87= 114553,82 руб.

4.6 Выводы по разделу

1. При технико-экономическом обосновании разработки ставилась задача расчета затрат на проведение работ по разработке рекомендаций по

защите информации в беспроводной сети стандарта IEEE 802.11ax ООО «Медиа-техника» г. Ставрополь.

2. Учитывая, что практический результат разработки рекомендаций в итоге предполагает корректировку Политики информационной безопасности компании, в части касающихся мероприятий по защите, задача технико-экономического обоснования состояла в стоимостной оценке объекта интеллектуальной собственности, которым, по сути, является этот документ.

3. Алгоритм расчета предполагал поэтапную оценку стоимости объекта интеллектуальной собственности, к которому был отнесен документ. Временные затраты на разработку сведены в таблицы, а так же рассчитана ожидаемая величина затрат для каждого этапа и всей работы в целом.

3. Проведена оценка капитальных затрат, с учетом того, что затраты на приобретение и внедрение определяются на контрактной или договорной основе заказчиком и подрядчиком. Эта информация является конфиденциальной, поэтому в расчётах использованы цены на программное обеспечение и оборудование, размещённые поставщиками на информационных ресурсах в сети Интернет. При этом затраты на приобретение системного программного обеспечения отсутствуют, так как проект реализуется на програмных ресурсах компании, имеющей лицензии на программные продукты разработки. Итоговые расходы с учетом капитальных затрат и суммарных расходов составили 114553,82 рубля.

ЗАКЛЮЧЕНИЕ

В выпускной квалификационной работе решалась актуальная задача снижение рисков потери информации в организации, использующей перспективную беспроводную сеть стандарта IEEE 802.11ax.

Во введении определена актуальность разработки, цель, объект и предмет исследования, детализированы частные задачи исследования.

В первом разделе выпускной квалификационной работы проведен анализ системы управления компании и актуализированы угрозы потери информации. Для решения задач предоставления телекоммуникационных услуг и сервисов в компании создана организационно-штатная структура, которая адаптирована под реализуемые ею стратегии. Особенности информационных технологий работы с информацией в компании связаны с одновременным использованием как информационной, так и технологической системами. При этом, как показал анализ отдельного структурного подразделения, отвечающего за защиту информации нет. Эта задача возложена на администратора ИС. Сделан вывод о необходимости перехода на сетевые технологии, в том числе беспроводной передачи данных, с возможностями передачи большого объема информации и высокими скоростями. Такие возможности предоставляют беспроводные сети, функционирующие на базе перспективного протокола IEEE 802.11ax с встроенным механизмом защиты WPA3, которые требуют совершенствования процедур администрирования в интересах защиты информации, циркулирующей в этих сетях.

Во втором разделе работы проведен анализ защищенности перспективной беспроводной сети стандарта IEEE 802.11ax отмечено, что причиной эволюции стандарта Wi-Fi в 802.11ax стал такой важный тренд как «интернет вещей» и уже сегодня исключительно важной является проблема безопасного и простого подключения сотен или более электронных

устройств к корпоративной информационной системе в соответствии с их эксплуатационными, инженерными и технологическими потребностями.

В третьем разделе работы проведена разработка рекомендаций по защите корпоративной Wi-Fi сети стандарта IEEE 802.11ax. Отмечено, что функционирование беспроводной сети стандарта может осуществляться в пяти режимах, что помогает решить проблемы, которые могут возникнуть у предприятия сегодня, и позволяет подготовиться к тому, что будет завтра. Отмечено, что важным является конфигурирование беспроводной сети стандарта IEEE 802.11ax, которое реализуется на основе пяти основных шагов которые можно объединить в общую системную последовательность.

В разделе проведен обзор известных атак на персональные сети по протоколам безопасности, данные сведены в таблицу. На основе анализа механизмов защиты, встроенных в стандарт IEEE 802.11ax сформирован алгоритм действий администратора информационной системы, который был привязан к основным процессам функционирования сети. В алгоритме выделены наиболее значимые действия, реализуемые при контроле службой информационной безопасности.

В четвертом разделе работы проведено технико-экономическое обоснование разработки рекомендаций по защите информации в беспроводной сети. Учитывая, что практический результат разработки рекомендаций в итоге предполагает корректировку Политики информационной безопасности компании, в части касающихся мероприятий по защите, задача технико-экономического обоснования состояла в поэтапной стоимостной оценке объекта интеллектуальной собственности, которым, по сути, является этот документ. Осуществлен расчет временных затрат на разработку, а так же рассчитана ожидаемая величина затрат для каждого этапа и всей работы в целом. Проведена оценка капитальных затрат, с учетом того, что затраты на приобретение и внедрение определяются на контрактной или договорной основе заказчиком и подрядчиком. Итоговые расходы с учетом капитальных затрат составили 114553,82 руб.

Важным практическим результатом работы является возможность реализации разработанных рекомендаций по защите информации в перспективной беспроводной сети в конкретной организации города Ставрополя, решающей задачи своей экономической стратегии в условиях конкуренции на рынке телекоммуникационных услуг.

Разработанные рекомендации по защите информации в беспроводной сети внесены в раздел «Функционирование информационной системы компании» «Концепции информационной безопасности» телекоммуникационной компании ООО «Медиа-техника». Имеется АКТ об использовании выводов и рекомендаций на производстве.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1 Программа «Цифровая экономика. Россия 2024». — URL: https://data-economy.ru/ (дата обращения 30.04.2020).

2 Дорожная карта развития «сквозной» цифровой технологии «Технологии беспроводной связи». — URL: https://digital.gov.ru/ru/documents/6674/ (дата обращения 30.04.2020).

3 Устав ООО «Медиа-техника» г. Ставрополь.

4 Мыльник В.В., Титаренко Б.П. Исследование систем управления. — М.: Инфра-М, 2014. — 240 с.

5 Гришина Н.В. Комплексная система защиты информации на предприятии. – М.: Форум, 2014. – 240 с.

6 Завгородний В.А. Комплексная защита информации в компьютерных системах. – М.: Логос, 2003. – 264 с.

7 Wi-Fi Alliance — URL: https://www.wi-fi.org/discover-wi-fi (дата обращения 2.05.2020).

8 Стандарт IEEE 802.11ax — URL: http://www.ieee802.org/ (дата обращения 3.05.2020).

9 Федеральный закон от 27 июля 2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

10 Федеральный закон «О коммерческой тайне» от 29 .07.2004 г. №98-ФЗ.

11 Федеральный закон «О персональных данных» от 27.07. 2006 г. №152-ФЗ.

12 Федеральный закон «О техническом регулировании» от 27.12.2002 г. №184-ФЗ.

13 Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

14 «Доктрина информационной безопасности Российской Федерации» (Утв. Указ Президента РФ от 05.12.2016 г. № 646).

15 «Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» (Утв. Указ Президента РФ от 12.12. 2014г № К1274).

16 «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года» (утв. Президентом РФ 24.07.2013, №Пр-1753).

17 ГОСТ РО 0043-001-2010 «Защита информации. Обеспечение безопасности информации в ключевых системах информационной инфраструктуры. Термины и определения».

18 ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программа и методики аттестационных испытаний».

19 ГОСТР 57640 2017/ISO/IEC TS 33052:2016 Информационные технологии. Эталонная модель процесса (ЭМП) для управления информационной безопасностью.

20 Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (Утв. Гостехкомиссией в 2002 г).

21 Сборник временных методик оценки защищённости конфиденциальной информации от утечки по техническим каналам. (Утв. Гостехкомиссией в 2001 г)

22 Приказ ФСТЭК от 18.02.2013г №17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

23 Белорусов Д.И., Корешков М.С. WIFI-сети и угрозы информационной безопасности // Специальная техника. 2009. № 6. С. 2–6.

24 Борисов В.И., Щербаков В.Б., Ермаков С.А. Спектр уязвимостей беспроводных сетей стандарта IEEE 802.11 // Информация и безопасность. 2008. Т. 11. № 3. С. 431–434.

25 Владимиров А.А., Гавриленко К.В., Михайловский А.А. Wi-фу:

«боевые» приемы взлома и защиты беспроводных сетей. - М.: НТ Пресс, 2005. 464 с.

26 Гордейчик С.В., Дубровин В.В. Безопасность беспроводных сетей. - М.: Горячая линия-Телеком, 2008. 288 с.

27 Блог электронного журнала «Compass Security Network Computing AG». — URL: https://blog.compass-security (дата обращения 1.05.2020).

28 Дорофеев А.В. Тестирование на проникновение: демонстрация одной уязвимости или объективная оценка защищенности? // Защита информации. INSIDE, 2010. № 6. С. 72–73.

29 Зегжда Д.П., Коваленко С.Л. Проблемы безопасности беспроводных сетей семейства EEE 802.11a/b/g // Проблемы информационной безопасности. Компьютерные системы. 2006. № 2. С. 45–49.

30 Иващук И.Ю. Модель и метод построения семейства профилей защиты для беспроводной сети. - СПб.: Изд. СПбГУИТМО. 133 с.

31 Львович Я.Е., Фефилов И.И., Савинский П.Л., Кащенко Г.А. Выбор технологии построения защищенных сетей беспроводной связи // Информация и безопасность. 2009. Т. 12. № 2. С. 263–268.

32 Марков А.С., Фадин А.А., Цирлов В.Л. Средства и технологии анализа защищенности // Информатизация и информационная безопасность правоохранительных органов. - М.: Академия управления МВД России, 2011. С. 434–437.

33 Мерритт М., Поллино Д. Безопасность беспроводных сетей. - М.: ДМК Пресс, 2004. 288 с.

34 Пролетарский А.В., Баскаков И.В., Чирков Д.Н. Беспроводные сети Wi-Fi. - М.: БИНОМ, 2007. 178 с.

35 Ворона В.А. Комплексные интегрированные системы обеспечения безопасности: учебное пособие/ Ворона В.А., Тихонов В.А.— Электрон. текстовые данные.— М.: Горячая линия - Телеком, 2013.— 160 с.

36 Сердюк В. А. Организация и технологии защиты информации:

обнаружение и предотвращение информационных атак в автоматизированных системах предприятий. М.: ГУ-ВШЭ, 2013 — ISBN 978-5-7598-0698-1 — 576 с.

37 Конеев И.Р. Информационная безопасность предприятий. - СПб.: БХВ-Петербург, 2013.- 752 с.

38 Ярочкин В.И. Информационная безопасность. – М.: Академический Проект: Фонд "Мир", 2013. – 640 с.

39 Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: Инфра–М, Форум, 2010. – 592 с.

40 Грибунин В.Г., Чудовский В.В. Комплексная система защиты информации на предприятии. – М.: Издательский дом "Академия", 2014. – 416 с.

41 Галатенко. В А. Основы информационной безопасности: учеб. пособие / В.А. Галатенко - М: Интуит.ру «Интернет-университет информационных технологий», 2004 -264с.

42 Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия: Учебное пособие. – М.: Издательско-торговая корпорация «Дашков и Ко », 2004. – 336 с.

43 Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность/ С.А Петренко. С В. Симонов М: Академия АиТи: ДМК Пресс, 2004. – 384 с.

44 Петренко С.А Аудит безопасности luranrt /С.А. Петренко, А.А.Петренко - М: Академии АиТи: ДМК Пресс. 2002. - 438с.

45 Оценка субъектов интеллектуальной собственности. – URL: https://patentural.ru/zhurnal/oczenka-intellektualnoj-sobstvennosti/ (дата обращения: 10.05.20).

46 Оркина Е.А. Оценка стоимости интеллектуальной собственности. – М: Феникс, 2013. – 128 с.