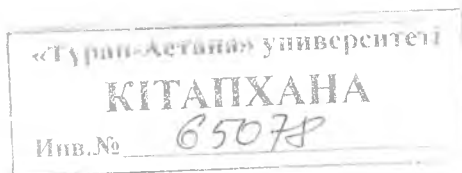


**М.З. Якубова, С.В. Коньшин, Р.Ш. Бердибаев,
О.А. Мананкова, А.К. Мукашева**

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебное пособие



Алматы, 2021

УДК 004.056.5(075.8)

ББК 32.972.53я73

К65

Рецензенты:

Кандидат технических наук, профессор кафедры информационной безопасности КазННТУ им. К.И.Сатпаева, **Е.Ж. Айтхожаева**.

Доктор технических наук, профессор кафедры Автоматизация и управление АУЭС, **Е.Т. Утепбергенов**.

Доктор PhD, зам.директора Центра Дистанционного обучения АЛИТ, **Д.Т. Касымова**.

М.З. Якубова, С.В. Коньшин, Р.Ш. Бердибаев, О.А. Мананкова,

А.К. Мукашева

К65 Основы информационной безопасности: Учебное пособие (для студентов всех специальностей)/М.З. Якубова, С.В. Коньшин, Р.Ш. Бердибаев, О.А. Мананкова, А.К. Мукашева. – Алматы: ТОО «Лантар Трейд», 2021. – 124 с.: табл. 3, ил.78, библиогр. - 38 назв.

ISBN 978-601-7939-83-0

В представленном учебном пособии обобщены, систематизированы и представлены сведения о конвергенции услуг телекоммуникации. Учебное пособие предназначено для студентов всех специальностей.

Учебное пособие содержит основные понятия об информационной безопасности систем, телекоммуникационных технологий, а так же основных методах и средствах защиты информационных ресурсов с применением современных виртуальных сред имитационного моделирования OpNet Modeler, Wireshark и Cryptedool2.

УДК 004.056.5(075.8)

ББК 32.972.53я73

Рекомендовано к изданию Ученым советом Алматинского университета энергетики и связи (Протокол № 11 от 20.04.2021 г.).

Печатается по тематическому плану выпуска ведомственной литературы АУЭС на 2021 год, позиция 9.

ISBN 978-601-7939-83-0

© М.З. Якубова, С.В. Коньшин,
Р.Ш. Бердибаев, О.А.Мананкова,
А.К. Мукашева, 2021

© ТОО «Лантар Трейд», 2021

Содержание

Введение	5
ГЛАВА 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	6
1.1 Этапы развития информационной безопасности	6
1.2 Понятие информационной безопасности	8
1.3 Концепция информационной безопасности	9
1.4 Уровни обеспечения информационной безопасности	12
1.4.1 Законодательный уровень	13
1.4.1 Административный уровень	17
1.4.2 Процедурный уровень	20
1.4.3 Программно-технический уровень	22
1.4.4 Достоинства и недостатки существующих мер обеспечения безопасности	25
Вопросы для самоконтроля:	26
ГЛАВА 2. КЛАССИФИКАЦИЯ УГРОЗ, УЯЗВИМОСТЕЙ И АТАК СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	28
2.1 Методика оценки угроз безопасности информационных систем и их уязвимостей	37
2.2 Системы обнаружения и предотвращения атак	45
2.3 Сканеры безопасности	48
Вопросы для самоконтроля	51
ГЛАВА 3. ПРАКТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ ПРОГРАММЫ CRYPTOOOL2	52
3.1 Освоение метода шифрования и дешифрования по алгоритму Цезаря в среде CrypTool2	52
3.1.1 Построение схемы Шифра Цезаря в среде CrypTool2	53
3.1.2 Частотный анализ	57
3.1.3 Взлом шифра Цезаря с помощью Brute Force	58
3.2 Исследование и криптоанализ алгоритма RSA	59
3.3 Реализация режимов шифрования алгоритма AES	62
3.3.1 Режим ECB	63
3.3.2 Реализация режима шифрования CBC на AES	69
3.3.3 Реализация режима шифрования CFB на AES	75
3.3.4 Реализация режима шифрования OFB на AES	79
ГЛАВА 4. ПРАКТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ ПРОГРАММ OPNET MODELER И WIRESHARK	86

4.1 Установка и изучение программной среды Opnet Modeler v.14 на примере проектирования локальной беспроводной сети и атаки на разработанную сеть с помощью Wireshark.	86
4.1.1 Настройка пользовательских приложений и их профилей.	95
4.1.2 Настройка сервера.	97
4.1.3 Настройка Маршрутизаторов беспроводного подключения.	99
4.1.4 Настройка Коммутаторов (Свитчей).	100
4.1.5 Настройка окончательных пользователей (рабочих станций – персональных компьютеров).	101
4.1.6 Настройка движения мобильных станций.	102
4.1.7 Настройка протокола сети.	102
4.1.8 Имитационное моделирование.	103
4.1.9 Проведение атаки с использованием Wireshark.	105
4.1.10 Захват сетевого трафика.	107
4.1.11 Фильтрация пакетов.	108
4.2 Проектирование глобальной беспроводной сети в программной среде Opnet Modeler v.14.5 и реализация атаки на разработанную сеть с помощью Wireshark.	112
4.2.1 Создание архитектуры беспроводной сети в Opnet.	112
4.2.2 Настройка оборудования сети, генерация трафика.	114
4.2.3 Реализация атаки на сеть.	116
Список литературы.	119

Введение

В настоящее время широко рассматривается вопрос обеспечения защиты информации в различных областях профессиональной деятельности, научной и практической работе, для самообразовательных и других целей.

Область обеспечения информационной безопасности телекоммуникационных систем и технологий имеет важность, как на социальном, так и на государственном уровне.

Своей задачей учебное пособие ставит освоение студентами знаний о понятиях информационной безопасности, методах и средствах построения безопасных систем телекоммуникаций, основных протоколах взаимодействия сетей и средств защиты информации, а также практического исследования этих процессов с использованием современных сред моделирования.

Наряду с практической целью, учебное пособие реализует образовательные и воспитательные цели, способствуя расширению кругозора студентов, повышению их общей культуры и образованности в области информационной безопасности.

ГЛАВА 1. ОСНОВНЫЕ ПОНЯТИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

1.1 Этапы развития информационной безопасности

Вопрос обеспечения безопасности информации возник с появлением средств информационных коммуникаций между людьми, а также с появлением интереса в обществе к ресурсам, которым может быть нанесен ущерб путём воздействия на них посредством информационных коммуникаций.

I этап (до 1816 года) характеризуется использованием естественно возникавших средств информационных коммуникаций. В этот период основная задача информационной безопасности заключалась в защите сведений о событиях, фактах, имуществе, местонахождении и других данных, имеющих для человека лично или сообщества, к которому он принадлежал, жизненное значение. Яркими примерами в области обеспечения безопасности с применением шифрования являются шифры Цезаря и Виженера;

II этап (с 1816 года) характеризуется началом использования искусственно создаваемых технических средств электро- и радиосвязи. Для обеспечения скрытности и помехозащищенности радиосвязи применяли помехоустойчивое кодирование сообщения (сигнала) с последующим декодированием принятого сообщения (сигнала);

III этап (с 1935 года) характеризуется появлением радиолокационных и гидроакустических средств. Основным способом обеспечения информационной безопасности в этот период было сочетание организационных и технических мер, направленных на повышение защищенности радиолокационных средств от воздействия на их приемные устройства активными маскирующими и пассивными имитирующими радиоэлектронными помехами;

IV этап (с 1946 года) характеризуется изобретением и внедрением в практическую деятельность электронно-вычислительных машин (компьютеров). Задачи информационной безопасности решались, в основном, методами и способами ограничения физического доступа к оборудованию средств добывания, переработки и передачи информации.

V этап (с 1965 года) обусловлен созданием и развитием локальных информационных сетей. Задачи информационной безопасности решались методами физической защиты, администрированием и управлением доступа к сетевым ресурсам. В этот период в связи с высокой скоростью обработки и передачи информации ЭВМ специалистами была предложена кодировка с помощью блочных шифров, более стойких и надёжных по сравнению с роторными системами, однако допускающих практическую реализацию только в виде цифровых электронных устройств;

VI этап (с 1973 года) характеризуется использованием расширением спектра коммуникационных устройств. Появлением сообществ людей - хакеров, которые ставят своей задачей нанести ущерб информационной безопасности отдельных пользователей, организаций и стран. На первый план выходит защита национальной безопасности, формируется правовая база.

В этот период формируется модель информационной безопасности, характеризующаяся тремя принципами, именуемыми триадой CIA (с англ. Confidentiality - «конфиденциальность», Integrity - «целостность», Availability - «доступность»). В 1977 году в Соединённых Штатах Америки был принят стандарт шифрования DES, разработанный компанией IBM, создателем и поставщиком аппаратного и программного обеспечения на мировой рынок. Этот стандарт лёг в основу многих современных криптосистем по всему миру;

VII этап (с 1985 года) связан с созданием и развитием глобальной телекоммуникационной сети Интернет с использованием космических средств связи. Целью обеспечения информационной безопасности с использованием пилотируемых космических систем является, разработка и эффективное использование комплексной информационной системы сбора, хранения, обработки, преобразования, передачи и реализации полученной космической информации. Приоритетное развитие космических систем различного целевого назначения является жизненно важным фактором обеспечения как национальной безопасности в целом, так и информационной безопасности в частности;

VIII этап (с 2011 года) – это этап современного развития, в котором информационная безопасность становится составной частью национальной безопасности. На современном этапе основная задача обеспечения безопасности – это своевременное совершенствование технико-технологических и информационных основ деятельности государственных и негосударственных организаций как внутри отдельно взятой страны, так и на международном уровне. Основой новой стратегии международной информационной безопасности должно стать взаимовыгодное сотрудничество государств в сфере международной информации, спектр которой охватывает все виды средств массовой информации и коммуникации (СМИиК), виды и направления информационных воздействий, объекты информационной безопасности, особенности сети Интернет как современной информационной системы и оружие разрушительных информационных действий.

1.2 Понятие информационной безопасности

В словаре стандарта ISO/IEC 2382:2015 «Информационные технологии» приводится такая трактовка:

Информация (в области обработки информации) – любые данные, представленные в электронной форме, написанные на бумаге, высказанные на совещании или находящиеся на любом другом носителе, используемые финансовым учреждением для принятия решений, перемещения денежных средств, установления ставок, предоставления ссуд, обработки операций и т.п., включая компоненты программного обеспечения системы обработки.

Для разработки концепции обеспечения информационной безопасности (ИБ) под информацией понимают сведения, которые доступны для сбора, хранения, обработки (редактирования, преобразования), использования и передачи различными способами, в том числе в компьютерных сетях и других информационных системах.

Такие сведения обладают высокой ценностью и могут стать объектами посягательств со стороны третьих лиц. Стремление оградить информацию от угроз лежит в основе создания систем информационной безопасности.

Прежде чем разрабатывать стратегию информационной безопасности, необходимо принять базовое определение самого понятия, которое позволит применять определенный набор способов и методов защиты.

Практики отрасли предлагают понимать под информационной безопасностью стабильное состояние защищенности информации, ее носителей и инфраструктуры, которая обеспечивает целостность и устойчивость процессов, связанных с информацией, к намеренным или непреднамеренным воздействиям естественного и искусственного характера. Воздействия классифицируются в виде угроз ИБ, которые могут нанести ущерб субъектам информационных отношений.

Таким образом, под защитой информации будет пониматься комплекс правовых, административных, организационных и технических мер, направленных на предотвращение реальных или предполагаемых ИБ-угроз, а также на устранение последствий инцидентов. Непрерывность процесса защиты информации должна гарантировать борьбу с угрозами на всех этапах информационного цикла: в процессе сбора, хранения, обработки, использования и передачи информации.

Информационная безопасность в этом понимании становится одной из характеристик работоспособности системы. В каждый момент времени система должна обладать измеряемым уровнем защищенности, и обеспечение безопасности системы должно быть непрерывным процессом, которые осуществляется на всех временных отрезках в период жизни системы.

1.3 Концепция информационной безопасности

ИБ-концепция для любой организации должны ответить на три основных вопроса:

- 1) Что защищать?
- 2) От кого защищать, какие виды угроз преваляют: внешние или внутренние?
- 3) Как защищать, какими методами и средствами?

В теории информационной безопасности под субъектами ИБ понимают владельцев и пользователей информации, причем пользователей не только на постоянной основе (сотрудники), но и пользователей, которые обращаются к базам данных в единичных

случаях, например, государственные органы, запрашивающие информацию. В ряде случаев, например, в банковских ИБ-стандартах к владельцам информации причисляют акционеров – юридических лиц, которым принадлежат определенные данные

Информационной угрозой в узком смысле признается объективная возможность воздействовать на объект защиты, которое может привести к утечке, хищению, разглашению или распространению информации. В более широком понимании к ИБ-угрозам будут относиться направленные воздействия информационного характера, цель которых – нанести ущерба государству, организации, личности. К таким угрозам относится, например, диффамация, намеренное введение в заблуждение, некорректная реклама.

Основные группы объектов защиты:

– информационные ресурсы всех видов (под ресурсом понимается материальный объект: жесткий диск, иной носитель, документ с данными и реквизитами, которые помогают его идентифицировать и отнести к определенной группе субъектов);

– права граждан, организаций и государства на доступ к информации, возможность получить ее в рамках закона; доступ может быть ограничен только нормативно-правовыми актами, недопустима организация любых барьеров, нарушающих права человека;

– система создания, использования и распространения данных (системы и технологии, архивы, библиотеки, нормативные документы);

– система формирования общественного сознания (СМИ, интернет-ресурсы, социальные институты, образовательные учреждения).

Каждый объект предполагает особую систему мер защиты от угроз ИБ и общественному порядку. Обеспечение информационной безопасности в каждом случае должно базироваться на системном подходе, учитывающем специфику объекта. Все это должно быть отражено в Концепции информационной безопасности организации – документе, который определяет меры и способы внедрения ИБ-системы для информационных систем организации.

Для управления информационной безопасностью и оценки ущерба используют характеристику приемлемости, таким

образом, ущерб определяется как приемлемый или неприемлемым. Каждой организации полезно утвердить собственные критерии допустимости ущерба в денежной форме или, например, в виде допустимого вреда репутации. В государственных учреждениях могут быть приняты другие характеристики, например, влияние на процесс управления или отражение степени ущерба для жизни и здоровья граждан. Критерии существенности, важности и ценности информации могут меняться в ходе жизненного цикла информационного массива, поэтому должны своевременно пересматриваться.

Спектр интересов субъектов, связанных с использованием информационных систем, можно разделить на следующие категории: обеспечение доступности, целостности и конфиденциальности информационных ресурсов и поддерживающей инфраструктуры. Иногда в число основных составляющих ИБ включают защиту от несанкционированного копирования информации, но, на наш взгляд, это слишком специфический аспект с сомнительными шансами на успех, поэтому мы не станем его выделять. Поясним понятия доступности, целостности и конфиденциальности:

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Под целостностью подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – это защита от несанкционированного доступа к информации. Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем её как важнейший элемент информационной безопасности. Особенно ярко ведущая роль доступности проявляется в разного рода системах управления – производством, транспортом и т.п. Внешне менее драматичные, но также весьма неприятные последствия – и материальные, и моральные – может иметь длительная недоступность

информационных услуг, которыми пользуется большое количество людей (продажа железнодорожных и авиабилетов, банковские услуги и т.п.).

Целостность можно подразделить на статическую (понимаемую как неизменность информационных объектов) и динамическую (относящуюся к корректному выполнению сложных действий (транзакций)). Средства контроля динамической целостности применяются, в частности, при анализе потока финансовых сообщений с целью выявления кражи, переупорядочения или дублирования отдельных сообщений. Целостность оказывается важнейшим аспектом ИБ в тех случаях, когда информация служит «руководством к действию». Рецептúra лекарств, предписанные медицинские процедуры, набор и характеристики комплектующих изделий, ход технологического процесса – все это примеры информации, нарушение целостности которой может оказаться в, буквальном смысле, смертельным. Неприятно и искажение официальной информации, будь то текст закона или страница Web-сервера какой-либо правительственной организации.

Конфиденциальность – самый проработанный у нас в стране аспект информационной безопасности. К сожалению, практическая реализация мер по обеспечению конфиденциальности современных информационных систем наталкивается в Казахстане на серьезные трудности. Во-первых, сведения о технических каналах утечки информации являются закрытыми, так что большинство пользователей лишено возможности составить представление о потенциальных рисках. Во-вторых, на пути пользовательской криптографии как основного средства обеспечения конфиденциальности стоят многочисленные законодательные препоны и технические проблемы.

1.4 Уровни обеспечения информационной безопасности

В деле обеспечения информационной безопасности успех может принести только комплексный подход. Для защиты интересов субъектов информационных отношений необходимо сочетать меры следующих уровней:

- законодательного;
- административного (приказы и другие действия руководства организаций, связанных с защищаемыми информационными системами);
- процедурного (меры безопасности, ориентированные на людей);
- программно-технического.

1.4.1 Законодательный уровень

Законодательный уровень является важнейшим для обеспечения информационной безопасности, так как большинство людей не совершают противоправных действий не потому, что это технически невозможно, а потому, что это осуждается и/или наказывается обществом, потому, что так поступать не принято.

На законодательном уровне можно выделить две группы мер:

- меры, направленные на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности (назовем их мерами ограничительной направленности);
- направляющие и координирующие меры, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности (меры созидательной направленности).

Самое важное на законодательном уровне – это создать механизм, позволяющий согласовать процесс разработки законов в соответствии с прогрессом информационных технологий. Законы не могут опережать жизнь, но важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению информационной безопасности.

Государственная политика в области обеспечения информационной безопасности Республики Казахстан (далее — государственная политика) является открытой и предусматривает информированность общества о деятельности государственных органов и общественных институтов в области информационной

безопасности с учетом ограничений, предусмотренных действующими законодательными актами Республики Казахстан. Она основывается на обеспечении прав физических и юридических лиц на свободное создание, поиск, получение и распространение информации любым законным способом.

Государство исходит из того, что информационные ресурсы являются объектом собственности, и способствует введению их в хозяйственный оборот при соблюдении законных интересов собственников, владельцев и распорядителей информационных ресурсов.

Государство считает приоритетным развитие современных информационных и телекоммуникационных технологий и технических средств, способных обеспечить создание национальных телекоммуникационных сетей и международный информационный обмен.

Государственная политика не допускает монополизма государственных органов и организаций в области обеспечения информационной безопасности, за исключением сферы защиты государственных секретов.

Происходящие в настоящее время процессы преобразования в политической жизни и экономике Казахстана оказывают непосредственное влияние на состояние его информационной безопасности.

Анализ современного состояния информационной безопасности в Казахстане показывает, что ее уровень в настоящее время не соответствует потребностям человека, общества и государства.

В этих целях необходима комплексная координация мер по защите информации в общегосударственном масштабе и на ведомственном уровне для обеспечения целостности и конфиденциальности информации.

С возрастанием роли Интернета в информационном пространстве возникает необходимость защиты прав и свобод человека и общества от информации, пропагандирующей насилие и жестокость, навязывания им ложной и недостоверной информации. При этом источники внешних угроз могут находиться вне юрисдикции законодательства Республики Казахстан, что существенно затрудняет применение системы правовых мер.

Актуальной проблемой является отсутствие отечественных информационных технологий, что вынуждает массового потребителя приобретать импортную технику, не имеющую подтверждения соответствия требованиям информационной безопасности. Это представляет угрозу информационной безопасности баз и банков данных, а также возможной зависимости страны от иностранных производителей компьютерной и телекоммуникационной техники и информационной продукции.

С точки зрения создания и использования информации субъекты информационных отношений могут выступать в качестве авторов, собственников, владельцев или пользователей.

Информация и информационные ресурсы могут являться вещной или интеллектуальной собственностью. Поэтому при обработке информации в информационных системах требуется обеспечивать не только конфиденциальность информации, но также ее целостность и доступность. Для электронных документов необходимо подтверждать электронной цифровой подписью подлинность каждого документа.

В отношении информации, содержащей сведения, составляющие государственные секреты, действует установленный режим секретности для всех субъектов отношений. Собственником данной информации является государство.

Для обеспечения защиты информации с ограниченным доступом, собственником которой является государство, функционирует государственная система защиты информации.

При формировании единого информационного пространства Республики Казахстан возрастает роль «электронного правительства», создание которого было предусмотрено Государственной программой формирования «электронного правительства» в Республике Казахстан на 2005-2007 годы, утвержденной Указом Президента Республики Казахстан от 10 ноября 2004 года № 1471. «Электронное правительство» позволит существенно повысить эффективность функционирования всех ветвей власти за счет обеспечения информационной поддержки их деятельности и динамичной организации информационного взаимодействия между ними, а также с субъектами экономики и населением.

В рамках Государственной программы формирования «электронного правительства» в Республике Казахстан на 2005-2007 годы создаются государственные базы данных «Физические лица», «Юридические лица», «Регистр недвижимости», «Адресный регистр», безопасность которых будет обеспечена в результате защищенного информационного взаимодействия между субъектами информационных отношений.

Основополагающим среди законов РК, посвященных вопросам информационной безопасности, следует считать закон «Об информации, информатизации и защите информации». В нем даются основные определения и намечаются направления развития законодательства в данной области.

Закон выделяет следующие цели защиты информации:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;

- предотвращение угроз безопасности личности, общества, государства;

- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;

- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации как объекта собственности;

- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;

- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

- обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

К основным законодательным актам, которые также регулируют правоотношения в области ИТ относятся:

1. Предпринимательский кодекс Республики Казахстан от 29 октября 2015 года;

2. Кодекс Республики Казахстан об административных правонарушениях от 5 июля 2014 года;

К Законам Республики Казахстан относятся:

1. «О связи» от 5 июля 2004 года;

2. «Об информатизации» от 24 ноября 2015 года;

3. «О телерадиовещании» от 18 января 2012 года;

4. «О техническом регулировании» от 9 ноября 2004 года;

5. «Об обеспечении единства измерений» от 7 июня 2000 года;

6. «О естественных монополиях и регулируемых рынках» от 9 июля 1998 года.

В отрасли инфокоммуникаций РК функционируют два технических комитета по стандартизации:

1. ТК 34 «Информационные технологии» на базе ОЮЛ «Казахстанская Ассоциация IT –компаний»;

2. ТК 63 «Системы, средства и услуги инфокоммуникаций» на базе ОЮЛ «Национальная телекоммуникационная ассоциация Казахстана».

Технические комитеты по стандартизации принимают участие в разработке национальных, предварительных национальных, международных, региональных, межгосударственных стандартов, а также в формировании программы национальной стандартизации

Так же в Казахстане утверждены национальные стандарты в области SmartCity. И действуют стандарты ИСО, среди которых ISO/IEC 27031:2011

«Информационные технологии. Методы обеспечения защиты. Руководящие указания по готовности информационно-коммуникационных технологий для ведения бизнеса», который описывает концепции и принципы готовности информационно-коммуникационных технологий (ИКТ) к обеспечению непрерывности бизнеса (ОНБ), и предоставляет систему методов и процессов готовности ИКТ любой организации к обеспечению непрерывности бизнеса.

1.4.1 Административный уровень

Законы и стандарты в области информационной безопасности служат лишь отправным нормативным базисом информационной безопасности. Т.У. Основой же практического

построения комплексной системы безопасности является административный уровень, определяющий главные направления работ по защите информационных систем.

Задача административного уровня – это разработка и реализация практических мероприятий по созданию системы информационной безопасности, учитывающей особенности защищаемых информационных систем.

Целью административного уровня является разработка программы работ в области информационной безопасности и обеспечение ее выполнения в конкретных условиях функционирования информационной системы.

Содержанием административного уровня являются следующие мероприятия:

- 1) разработка политики безопасности;
- 2) проведение анализа угроз и расчета рисков;
- 3) выбор механизмов и средств обеспечения информационной безопасности.

Политика информационной безопасности – комплекс основных мер по защите информации, в том числе информации с ограниченным распространением (служебная информация), информационных процессов и включает в себя требования в адрес пользователей информационных систем организации, его ведомств и подведомственных организаций в своей деятельности.

Выбор нормативной базы, на которой строится разработка политики, зависит от того, в каком правовом поле и деловой среде преимущественно работает организация.

К категории средств обеспечения информационной безопасности представлена законодательными актами и нормативно-распорядительными документами, которые действуют на уровне организации.

В мировой практике при разработке нормативных средств ориентируются в работе по подготовке политики информационной безопасности на такие нормативные акты, как ISO/IEC 27001-2005, ISO/IEC 17799-2005, ISO/IEC 27000-2016, ISO/IEC TR 13335.

Стандарты создавали две организации:

ISO – Международная комиссия по стандартизации, которая разрабатывает и утверждает большинство признанных на

международном уровне методик сертификации качества процессов производства и управления;

IEC – Международная энергетическая комиссия, которая внесла в стандарт свое понимание систем ИБ, средств и методов ее обеспечения

Актуальная версия ISO/IEC 27000-2016 предлагают готовые стандарты и опробованные методики, необходимые для внедрения ИБ. По мнению авторов методик, основа информационной безопасности заключается в системности и последовательной реализации всех этапов от разработки до пост-контроля.

Для получения сертификата, который подтверждает соответствие стандартам по обеспечению информационной безопасности, необходимо внедрить все рекомендуемые методики в полном объеме. Если нет необходимости получать сертификат, в качестве базы для разработки собственных ИБ-систем допускается принять любую из более ранних версий стандарта, начиная с ISO/IEC 27000-2002, или российских ГОСТов, которые носят рекомендательный характер.

По итогам изучения стандарта разрабатываются два документа, которые касаются безопасности информации. Основной, но менее формальный – концепция ИБ предприятия, которая определяет меры и способы внедрения ИБ-системы для информационных систем организации. Второй документ, которые обязаны исполнять все сотрудники организации, – положение об информационной безопасности, утверждаемое на уровне совета директоров или исполнительного органа.

Кроме положения на уровне организации должны быть разработаны перечни сведений, составляющих коммерческую тайну, приложения к трудовым договорам, закрепляющий ответственность за разглашение конфиденциальных данных, иные стандарты и методики. Внутренние нормы и правила должны содержать механизмы реализации и меры ответственности. Чаще всего меры носят дисциплинарный характер, и нарушитель должен быть готов к тому, что за нарушением режима коммерческой тайны последуют существенные санкции вплоть до увольнения.

В рамках административной деятельности по защите ИБ анализ и оценка рисков должны проводиться в соответствии с

руководством по реализации стандарта ИСО/МЭК 27001-2008 «Информационная технология. Методы и средства обеспечения безопасности. Системы управления информационной безопасностью. Требования». При оценке рисков должно учитываться влияние реализации угроз информационной безопасности на количественные и качественные показатели. Стоимость принимаемых мер не должна превышать возможный ущерб, возникающий при реализации угроз. Реализуемые в разумно достаточном объеме меры и мероприятия по обеспечению информационной безопасности должны сводить риски к минимуму, при этом адекватность и эффективность защитных мер должна быть оцениваема на регуляторной основе.

Выбор механизмов и средств обеспечения информационной безопасности определяется организацией самостоятельно. В качестве методов обеспечения информационной безопасности могут выступать меры по защите переговорных комнат и кабинетов руководства от прослушивания, и установление различных уровней доступа к информации (п.1.4.3).

1.4.2 Процедурный уровень

К процедурным мерам обеспечения информационной безопасности в первую очередь относится разработка положений, регламентов и процессов взаимодействия. Принятие некоторых внутренних нормативных актов регламентируется требованиями законодательства.

Мероприятия по защите информации на процедурном уровне включают в себя:

- документирование и оптимизацию бизнес-процессов;
- установку градации сотрудников и их уровней доступа к информации, содержащей коммерческую тайну;
- создание подразделений или назначение лиц, ответственных за обеспечение информационной безопасности, иногда изменение структуры предприятия в соответствии с требованиями безопасности;
- информирование или переобучение персонала;
- организацию мероприятий по тестированию подготовки персонала к работе с системой в критических ситуациях;

– получение лицензий, например, на работу с государственной тайной;

– обеспечение технической защиты помещений и оборудования с дальнейшей сертификацией классов защиты, определение их соответствия нормативно-правовым требованиям;

– создание системы безопасности для цепочки поставщиков, во взаимодействии с которыми передаются конфиденциальные данные, внесение в договоры с контрагентами оговорок о сохранении коммерческой тайны и мер ответственности за ее разглашение;

– установка пропускной системы для сотрудников, выдача им электронных средств идентификации;

– выполнение всех требований законодательства по защите персональных данных;

– разработка системы взаимодействия с государственными органами в случае запроса ими у организации информации, которая может быть отнесена к конфиденциальной;

– регламентацию деятельности персонала на допуск к интернету, внешней электронной почте, другим ресурсам;

– получение электронной цифровой подписи для усиления безопасности финансовой и другой информации, которую передают государственным органам по каналам электронной почты.

Морально-этические меры определяют личное отношение человека к конфиденциальной информации или информации, ограниченной в обороте. Повышение уровня знаний сотрудников касательно влияния угроз на деятельность организации влияет на степень сознательности и ответственности сотрудников. Чтобы бороться с нарушениями режима информации, включая, например, передачу паролей, неосторожное обращение с носителями, распространение конфиденциальных данных в частных разговорах, требуется делать упор на личную сознательность сотрудника. Полезным будет установить показатели эффективности персонала, которые будут зависеть от отношения к корпоративной системе ИБ.

1.4.3 Программно-технический уровень

Широкий диапазон технических средств ИБ-защиты включает:

1) Физические средства защиты. Это механические, электрические, электронные механизмы, которые функционируют независимо от информационных систем и создают препятствия для доступа к ним. Замки, в том числе электронные, экраны, жалюзи призваны создавать препятствия для контакта дестабилизирующих факторов с системами. Группа дополняется средствами систем безопасности, например, видеокамерами, видеорегистраторами, датчиками, выявляющие движение или превышение степени электромагнитного излучения в зоне расположения технических средств снятия информации, закладных устройств.

2) Аппаратные средства защиты. Это электрические, электронные, оптические, лазерные и другие устройства, которые встраиваются в информационные и телекоммуникационные системы. Перед внедрением аппаратных средств в информационные системы необходимо удостовериться в совместимости.

3) Программные средства – это простые и системные, комплексные программы, предназначенные для решения частных и комплексных задач, связанных с обеспечением ИБ. Примером комплексных решений служат DLP-системы и SIEM-системы: первые служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков, вторые – обеспечивают защиту от инцидентов в сфере информационной безопасности. Программные средства требовательны к мощности аппаратных устройств, и при установке необходимо предусмотреть дополнительные резервы.

В качестве тривиальных программных систем защиты так же может выступать антивирусные программы для стационарных устройств и облачные антивирусы. CloudAV – это одно из облачных решений информационной безопасности, что применяет легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдера. CloudAV – это также решение для эффективного сканирования вирусов на приспособлениях с невысокой вычислительной мощностью для

выполнения самих сканирований. Некоторые образцы облачных антивирусных программ – это Panda Cloud Antivirus, CrowdStrike, Cb Defense и Immunet.

4) К специфическим средствам информационной безопасности относятся различные криптографические алгоритмы (DES – Data Encryption Standard, AES – Advanced Encryption Standard, RSA – Rivest, Shamir, Adelman), позволяющие шифровать информацию на диске и перенаправляемую по внешним каналам связи и между другими полезными приложениями, включая улучшенные методы проверки подлинности, дайджесты сообщений, цифровые подписи и зашифрованные сетевые коммуникации. Преобразование информации может происходить при помощи программных и аппаратных методов, работающих в корпоративных информационных системах. Беспроводная связь может быть зашифрована с использованием таких протоколов, как WPA/WPA2 или более старый (и менее безопасный) WEP. Проводные коммуникации (такие как ITU-T G.hn) защищены с использованием AES для шифрования и X.1035 для аутентификации и обмена ключами. Программные приложения, такие как GnuPG или PGP, могут применяться для шифрования информационных файлов и электронной почты.

5) Межсетевые экраны (брандмауэры или файрволы) – устройства контроля доступа в сеть, предназначенные для блокировки и фильтрации сетевого трафика. Брандмауэры обычно классифицируются как сетевые или хост-серверы. Сетевые брандмауэры на базе сети расположены на шлюзовых компьютерах LAN, WAN и интрасетях. Это либо программные устройства, работающие на аппаратных средствах общего назначения, либо аппаратные компьютерные устройства брандмауэра. Брандмауэры предлагают и другие функции для внутренней сети, которую они защищают, например, являются сервером DHCP или VPN для этой сети. Одними из лучших решений как для малых, так и для больших предприятий являются межсетевые экраны компаний Cisco Systems, CheckPoint, FortiGate, CyberGuard и др.

6) Виртуальная частная сеть (VPN - Virtual Private Network) дает возможность определить и использовать для передачи и получения информации частную сеть в рамках общедоступной

сети. Таким образом, приложения, работающие по VPN, являются надежно защищенными. VPN дает возможность подключиться к внутренней сети на расстоянии. С помощью VPN можно создать общую сеть для территориально отдаленных друг от друга предприятий. Что касается отдельных пользователей сети – они также имеют свои преимущества использования VPN, так как могут защищать собственные действия с помощью VPN, а также избегать территориальные ограничения и использовать прокси-серверы, чтобы скрыть свое местоположение.

7) Проxy-server (Прокси-сервер) – это определенный компьютер или компьютерная программа, которая является связывающим звеном между двумя устройствам, например, такими как компьютер и другой сервер. Прокси-сервер можно установить на одном компьютере вместе с сервером брандмауэра, или же на другом сервере. Плюсы прокси-сервера в том, что его кэш может служить для всех пользователей. Интернет-сайты, которые являются наиболее часто запрашиваемыми, чаще всего находятся в кэше прокси, что несомненно удобно для пользователя. Фиксирование своих взаимодействий прокси-сервером служит полезной функцией для исправления неполадок.

8) Для контроля мобильных устройств сотрудников и защиты данных организации необходимо внедрение специальных решений, таких как VMware AirWatch, IBM MaaS360, Blackberry Enterprise Mobility Suite, VMware Workspace One.

Все средства, гарантирующие безопасность информации, должны использоваться в совокупности, после предварительной оценки ценности информации и сравнения ее со стоимостью ресурсов, затраченных на охрану. Поэтому предложения по использованию средств должны формулироваться уже на этапе разработки систем, а утверждение должно производиться на том уровне управления, который отвечает за утверждение бюджетов.

В целях обеспечения безопасности необходимо проводить мониторинг всех современных разработок, программных и аппаратных средств защиты, угроз и своевременно вносить изменения в собственные системы защиты от несанкционированного доступа. Только адекватность и оперативность реакции на угрозы поможет добиться высокого уровня конфиденциальности в работе организации.

1.4.4 Достоинства и недостатки существующих мер обеспечения безопасности

Законодательные и морально-этические меры противодействия, являются универсальными в том смысле, что принципиально применимы для всех каналов проникновения и НСД к КС и информации. В некоторых случаях они являются единственно применимыми, как например, при защите открытой информации от незаконного тиражирования или при защите от злоупотреблений служебным положением при работе с информацией.

Организационные меры играют значительную роль в обеспечении безопасности компьютерных систем. Организационные меры - это единственное, что остается, когда другие методы и средства защиты отсутствуют или не могут обеспечить требуемый уровень безопасности. Однако, это вовсе не означает, что систему защиты необходимо строить исключительно на их основе, как это часто пытаются сделать чиновники, далекие от технического прогресса.

Этим мерам присущи серьезные недостатки, такие как:

- низкая надежность без соответствующей поддержки физическими, техническими и программными средствами (люди склонны к нарушению любых установленных дополнительных ограничений и правил, если только их можно нарушить);

- дополнительные неудобства, связанные с большим объемом рутинной и формальной деятельности.

Организационные меры необходимы для обеспечения эффективного применения других мер и средств защиты в части, касающейся регламентации действий людей. В то же время организационные меры необходимо поддерживать более надежными физическими и техническими средствами.

Физические и технические средства защиты призваны устранить недостатки организационных мер, поставить прочные барьеры на пути злоумышленников и в максимальной степени исключить возможность неумышленных (по ошибке или халатности) нарушений регламента со стороны персонала и пользователей системы.

Даже при допущении возможности создания абсолютно надежных физических и технических средств защиты, перекрывающих все каналы, которые необходимо перекрыть,

всегда остается возможность воздействия на персонал системы, осуществляющий необходимые действия по обеспечению корректного функционирования этих средств (администратора КС, администратора безопасности и т.п.). Вместе с самими средствами защиты эти люди образуют так называемое «ядро безопасности». В этом случае, стойкость системы безопасности будет определяться стойкостью персонала из ядра безопасности системы, и повышать ее можно только за счет организационных (кадровых) мероприятий, законодательных и морально-этических мер.

Но даже имея совершенные законы и проводя оптимальную кадровую политику, все равно проблему защиты до конца решить не удастся.

Во-первых, потому, что вряд ли удастся найти персонал, в котором можно было быть абсолютно уверенным, и в отношении которого невозможно было бы предпринять действий, вынуждающих его нарушить запреты.

Во-вторых, даже абсолютно надежный человек может допустить случайное, неумышленное нарушение.

Вопросы для самоконтроля:

1. Что такое информационная безопасность?
2. Основные этапы развития информационной безопасности.
3. Что является целью концепции обеспечения ИБ?
4. Понятие целостности информации?
5. Что такое доступность информации?
6. Что такое конфиденциальность информации?
7. Что собой представляют объекты ИБ?
8. Основные группы объектов защиты. Классификация.
9. Что собой представляют субъекты ИБ?
10. Что такое Концепция информационной безопасности?
11. Обзор законодательства РК в области информационной безопасности.
12. Основные положения Закона «Об информации, информатизации и защите информации».
13. Достоинства и недостатки существующих мер обеспечения безопасности.
14. Какие физические средства защиты существуют.

15. Понятие программных средств. Классификация.
16. Какие системы служат для предотвращения утечки, переформатирования информации и перенаправления информационных потоков.
17. Современные антивирусные программы для стационарных устройств и облачные антивирусы.
18. Основные средства криптографической информационной безопасности.
19. Какими средствами обеспечивается защита беспроводной связи?
20. Понятие и применение межсетевых экранов.
21. Понятие виртуальной частной сети (VPN - Virtual Private Network).
22. Современные средства контроля мобильных систем.
23. Основные нормативные акты ISO/IEC 27001-2005, ISO/IEC 17799-2005, ISO/IEC 27000-2016, ISO/IEC TR 13335. Понятие. Основные принципы.

2 КЛАССИФИКАЦИЯ УГРОЗ, УЯЗВИМОСТЕЙ И АТАК СИСТЕМ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Под угрозой безопасности понимают потенциально опасные воздействия на систему, которые прямо или косвенно наносят вред пользователю. Непосредственную реализацию угрозы называют атакой.

Угрозы информационной безопасности проявляются не самостоятельно, а через возможное взаимодействие с наиболее слабыми звеньями системы защиты, то есть через факторы уязвимости. Угроза приводит к нарушению деятельности систем на конкретном объекте-носителе.

Знания о возможных угрозах и уязвимых местах защиты, которые эти угрозы обычно эксплуатируют, необходимы для выбора наиболее экономичных средств обеспечения безопасности.

Существуют неумышленные и умышленные угрозы.

Неумышленные угрозы связаны с ошибками оборудования или программного обеспечения; ошибками человека; форс-мажорными обстоятельствами.

Умышленные угрозы преследуют цель нанесения ущерба пользователям информационных систем и подразделяются на активные и пассивные. Пассивная угроза – это несанкционированный доступ к информации без изменения состояния системы, активная – связана с попытками перехвата и изменения информации.

Несанкционированный доступ (НСД) заключается в получении пользователем доступа к ресурсу, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности.

Так же распространены такие угрозы как «отказ в услуге», который представляет собой преднамеренную блокировку легального доступа к информации и другим ресурсам; незаконное использование привилегий; «вирус» – это программа, способная заражать другие программы, путем модификации их так, чтобы они включали в себя копию вируса; «тройанский конь» – это программа, содержащая скрытый или явный программный код, при исполнении которого нарушается функционирование системы безопасности; «червяк» – это программа, которая

распространяется в системах и сетях по линиям связи. Такие программы подобны вирусам: заражают другие программы, а отличаются от вирусов тем, что не способны самовоспроизводиться; «лазейки» – точка входа в программу, благодаря которой открывается доступ к некоторым системным функциям. Обнаруживается путем анализа работы программы и др.

К классу вредоносных программ можно отнести снифферы (программы, перехватывающие сетевые пакеты), программы подбора паролей, атаки на переполнение буфера, в некоторых приложениях - дизассемблеры и отладчики.

Классификация угроз информационной безопасности:

- хищение (копирование) информации;
- модификация (искажение) информации;
- нарушение доступности (блокирование) информации;
- отрицание подлинности информации;
- навязывание ложной информации;
- потеря данных;
- мошенничество;
- кибервойны;
- кибертерроризм.

Хищение – это совершенные с корыстной целью противоправные безвозмездное изъятие и (или) обращение чужого имущества в пользу виновного или других лиц, причинившее ущерб собственнику или владельцу имущества.

Копирование компьютерной информации - повторение и устойчивое запечатление информации на машинном или ином носителе.

Уничтожение - внешнее воздействие на имущество, в результате которого оно прекращает свое физическое существование либо приводятся в полную непригодность для использования по целевому назначению. Уничтоженное имущество не может быть восстановлено путем ремонта или реставрации и полностью выводится из хозяйственного оборота.

Повреждение - изменение свойств имущества при котором существенно ухудшается его состояние, утрачивается значительная часть его полезных свойств и оно становится

полностью или частично непригодным для целевого использования.

Модификация компьютерной информации - внесение любых изменений, кроме связанных с адаптацией программы для ЭВМ или баз данных.

Блокирование компьютерной информации - искусственное затруднение доступа пользователей к информации, не связанное с ее уничтожением.

Несанкционированное уничтожение, блокирование модификация, копирование информации - любые не разрешенные законом, собственником или компетентным пользователем указанные действия с информацией.

Обман (отрицание подлинности, навязывание ложной информации) - умышленное искажение или сокрытие истины с целью ввести в заблуждение лицо, в ведении которого находится имущество и таким образом добиться от него добровольной передачи имущества, а также сообщение с этой целью заведомо ложных сведений.

Потеря данных (Data Loss) — повреждение или утрата информации в результате влияния различных факторов, случайных или намеренных действий. Потерять данные можно во время работы с ними, а также при хранении информации на компьютере, сервере или на массивах RAID. Потеря данных (Data Loss) может происходить в результате: нарушения целостности информации (сбой программного обеспечения) или неисправности оборудования.

Мошенничество, или фрод (англ. fraud — «мошенничество») — вид незаконного использования информационных технологий в различных областях бизнеса, от телекоммуникаций до банковского сектора, цель которого обычно состоит в том, чтобы присвоить денежные средства жертвы. Для фрода кибермошенники могут использовать множество методов: фишинг, скимминг, социальную инженерию, кардинг, «нигерийские письма» и т.п.

При фишинге хакеры пытаются всеми способами получить от пользователя его личные данные, логины и пароли. Мошенники могут создавать поддельные сайты, внешне неотличимые от настоящих, с похожими доменными именами, чтобы пользователь поверил в их подлинность и попытался

пройти авторизацию со своим логином и паролем, после чего учетные данные окажутся у злоумышленников. Также фишинг может быть реализован в виде электронных писем и других подобных сообщений, в которых мошенники от имени компании (банка, социальной сети и т.п.) запрашивают у пользователя сведения для входа в аккаунт или его личные данные (номера кредитных карт, копии документов).

Кража личности — преступление, при котором один человек выдает себя за другого. Мошенники могут делать это, например, для того, чтобы удаленно получить кредит на чужое имя. По информации исследователей, работающих в области безопасности, на черном рынке полный комплект данных для кражи личности (включая документы) стоит 16-30 долларов США.

Кардинг - это кража данных о пластиковых картах и их владельцах (адрес, ответы на секретные вопросы, дата рождения, имя) для последующей оплаты товара в интернет-магазинах или продажи на черном рынке.

Для получения данных мошенники применяют фишинг, социальную инженерию, специальные устройства, особые виды вредоносных программ. Также они могут получать сведения после взлома интернет-магазинов или банков. Для получения данных о реквизитах платежной карты мошенники могут устанавливать специальные устройства на банкоматы. Эти устройства считывают данные с карточки и пин-код, который вводит пользователь. Также злоумышленники могут устанавливать специальные программы на взломанные банкоматы, киоски оплаты, POS-терминалы.

Часто мошенники используют специальные устройства для кражи информации с магнитной ленты платежной карты. Такой вид мошенничества называется скиммингом. Скиммеры с помощью специального оборудования могут перенести данные одной платежной карты на другую. С появлением бесконтактных карт оплаты скиммеры стали использовать новое оборудование для считывания данных с них.

Кибервойны (Cyberwarfare) — это военные действия, осуществляемые не физически, а электронно, когда в качестве оружия выступает информация, а инструментами являются компьютеры и интернет. Кибервойна, таким образом, является

одним из видов информационной войны, задача которой — достичь определенных целей в экономической, политической, военной и других областях посредством воздействия на общество и власть тщательно подготовленной информацией.

Кибернетическая война состоит из двух этапов: шпионаж и атаки. Первый этап подразумевает сбор данных посредством взлома компьютерных систем других государств. Атаки можно разделить на типы в зависимости от цели и задач военных действий:

1) Вандализм — размещение пропагандистских или оскорбительных картинок на веб-страницах вместо исходной информации.

2) Пропаганда и информационная война — использование пропаганды в контенте веб-страниц, в почтовых и других подобных рассылках.

3) Утечки конфиденциальных данных — все, что представляет интерес, копируется со взломанных частных страниц и серверов, также секретные данные могут быть подменены.

4) DDoS-атаки — поток запросов со множества машин с целью нарушить функционирование сайта, системы компьютерных устройств.

5) Нарушение работы компьютерной техники — атаке подвергаются компьютеры, отвечающие за функционирование оборудования военного или гражданского назначения. Нападение приводит к выходу техники из строя или к ее отключению.

6) Атаки на инфраструктурные и критически важные объекты и кибертерроризм — воздействие на машины, которые регулируют инженерные, телекоммуникационные, транспортные и другие системы, обеспечивающие жизнедеятельность населения.

Кибертерроризм — комплекс незаконных действий в киберпространстве, создающих угрозу государственной безопасности, личности и обществу. Может привести к порче материальных объектов, искажению информации или другим проблемам.

Основной целью кибертерроризма является влияние на решение социальных, экономических и политических задач. В мире стремительно растет количество «умных» устройств

интернета вещей. Все они дают почву для целенаправленных атак с целью террора или шантажа — тем более что сейчас даже многие заводы и фабрики используют такие устройства в автоматизированных системах управления технологическим процессом (АСУ ТП). Киберпреступники могут взломать их с целью террора населения: например, организовать вывод цеха из строя или даже взрыв АЭС.

В своих акциях преступники активно используют все возможности современных технологий, в том числе современные гаджеты и программные продукты, радиоэлектронные устройства, достижения в других областях (вплоть до микробиологии и генной инженерии). Официально кибертерроризмом признаются акты, совершенные одним человеком или независимыми группами, состоящими из нескольких участников. Если в подпадающих под это определение действиях принимают участие представители правительств или иных государственных структур, это считается проявлениями кибервойны.

Действия кибертеррористов направлены на:

- взлом компьютерных систем и получение доступа к личной и банковской информации,
- военным и государственным конфиденциальным данным;
- вывод из строя оборудования и программного обеспечения, создание помех, нарушение работы сетей электропитания;
- кражу данных с помощью взлома компьютерных систем, вирусных атак, программных закладок;
- утечку секретной информации в открытый доступ;
- распространение дезинформации с помощью захваченных каналов СМИ;
- нарушение работы каналов связи и прочее.

Угрозы запускаются с целью получения незаконной выгоды вследствие нанесения ущерба информации. Но возможно и случайное действие угроз из-за недостаточной степени защиты и массового действия угрожающего фактора.

Основные уязвимости возникают по причине действия следующих факторов:

- несовершенство программного обеспечения, аппаратной платформы;
- разные характеристики строения автоматизированных систем в информационном потоке;
- разные характеристики строения автоматизированных систем в информационном потоке;
- часть процессов функционирования систем является неполноценной;
- неточность протоколов обмена информацией и интерфейса;
- сложные условия эксплуатации и расположения информации.

Существует разделение уязвимостей по классам, они могут быть:

- объективными;
- случайными;
- субъективными.

Если устранить или как минимум ослабить влияние уязвимостей, можно избежать полноценной угрозы, направленной на систему хранения информации.

Объективные уязвимости. Этот вид напрямую зависит от технического построения оборудования на объекте, требующем защиты, и его характеристик. Полноценное избавление от этих факторов невозможно, но их частичное устранение достигается с помощью инженерно-технических приемов, следующими способами:

1. Связанные с техническими средствами излучения:

- электромагнитные методики (побочные варианты излучения и сигналов от кабельных линий, элементов техсредств);
- звуковые варианты (акустические или с добавлением вибросигналов);
- электрические (проскальзывание сигналов в цепочки электрической сети, по наводкам на линии и проводники, по неравномерному распределению тока).

2. Активизируемые:

- вредоносные ПО, нелегальные программы, технологические выходы из программ, что объединяется термином «программные закладки»;

– закладки аппаратуры – факторы, которые внедряются напрямую в телефонные линии, в электрические сети или просто в помещения.

3. Те, что создаются особенностями объекта, находящегося под защитой:

– расположение объекта (видимость и отсутствие контролируемой зоны вокруг объекта информации, наличие вибро- или звукоотражающих элементов вокруг объекта, наличие удаленных элементов объекта);

– организация каналов обмена информацией (применение радиоканалов, аренда частот или использование всеобщих сетей).

4. Те, что зависят от особенностей элементов-носителей:

– детали, обладающие электроакустическими модификациями (трансформаторы, телефонные устройства, микрофоны и громкоговорители, катушки индуктивности);

– вещи, подпадающие под влияние электромагнитного поля (носители, микросхемы и другие элементы).

Случайные уязвимости. Эти факторы зависят от непредвиденных обстоятельств и особенностей окружения информационной среды. Их практически невозможно предугадать в информационном пространстве, но важно быть готовым к их быстрому устранению. Устранить такие неполадки можно с помощью проведения инженерно-технического разбирательства и ответного удара, нанесенного угрозе информационной безопасности:

1. Сбои и отказы работы систем:

– вследствие неисправности технических средств на разных уровнях обработки и хранения информации (в том числе и тех, что отвечают за работоспособность системы и за контроль доступа к ней);

– неисправности и устаревания отдельных элементов (размагничивание носителей данных, таких как дискеты, кабели, соединительные линии и микросхемы);

– сбои разного программного обеспечения, которое поддерживает все звенья в цепи хранения и обработки информации (антивирусы, прикладные и сервисные программы);

– перебои в работе вспомогательного оборудования информационных систем (неполадки на уровне электропередачи).

2. Ослабляющие информационную безопасность факторы:

- повреждение коммуникаций вроде водоснабжения или электроснабжения, а также вентиляции, канализации;
- неисправности в работе ограждающих устройств (заборы, перекрытия в здании, корпуса оборудования, где хранится информация).

Субъективные уязвимости. Этот подвид в большинстве случаев представляет собой результат неправильных действий сотрудников на уровне разработки систем хранения и защиты информации. Поэтому устранение таких факторов возможно при помощи методик с использованием аппаратуры и ПО:

1. Неточности и грубые ошибки, нарушающие информационную безопасность:

- на этапе загрузки готового программного обеспечения или предварительной разработки алгоритмов, а также в момент его использования (возможно во время ежедневной эксплуатации, во время ввода данных);

- на этапе управления программами и информационными системами (сложности в процессе обучения работе с системой, настройки сервисов в индивидуальном порядке, во время манипуляций с потоками информации);

- во время пользования технической аппаратурой (на этапе включения или выключения, эксплуатации устройств для передачи или получения информации).

2. Нарушения работы систем в информационном пространстве:

- режима защиты личных данных (проблему создают уволенные работники или действующие сотрудники в нерабочее время, они получают несанкционированный доступ к системе);

- режима сохранности и защищенности (во время получения доступа на объект или к техническим устройствам);

- во время работы с техустройствами (возможны нарушения в энергосбережении или обеспечении техники);

- во время работы с данными (преобразование информации, ее сохранение, поиск и уничтожение данных, устранение брака и неточностей).

2.1 Методика оценки угроз безопасности информационных систем и их уязвимостей

Оценка уязвимости – это процесс определения, идентификации, классификации и ранжирования уязвимостей в компьютерных системах, приложениях и сетевой инфраструктуре, а также предоставление необходимых знаний, осведомленности и рисков для понимания угроз своей среде и подходящего реагирования.

Процесс оценки уязвимости, предназначенный для выявления угроз и рисков, которые они представляют, обычно включает использование инструментов автоматического тестирования, таких как сканеры сетевой безопасности, результаты которых перечислены в отчете оценки уязвимости.

Каждая уязвимость должна быть учтена и оценена специалистами. Поэтому важно определить критерии оценки опасности возникновения угрозы и вероятности поломки или обхода защиты информации. Показатели подсчитываются с помощью применения ранжирования.

Оптимальным методом анализа угроз является метод экспертных оценок, при котором экспертам предлагается оценить возможность реализации некоторого перечня угроз.

В качестве критериев оценки опасности конкретной угрозы выделяют:

- 1) Возможность возникновения источника угрозы (K1).
- 2) Степень его готовности произвести атаку (K2).
- 3) Фатальность для объекта от реализации угрозы (K3).

Фатальность – характеристика, которая оценивает глубину влияния уязвимости на возможности программистов справиться с последствиями созданной угрозы для информационных систем. Если оценивать только объективные уязвимости, то определяется их информативность – способность передать в другое место полезный сигнал с конфиденциальными данными без его деформации.

Коэффициент опасности угрозы вычисляется на основании баллов, выставленных экспертом по трем критериям, например, от 1 до 10, по следующей формуле:

$$K_{\text{опуг}} = \frac{K_1 K_2 K_3}{10^3} \quad (1)$$

Для N экспертов общий коэффициент опасности угрозы вычисляется как произведение средних баллов, выставленных экспертами по каждому критерию:

$$K_{\text{опуг}N} = \frac{\sum_{i=1}^N K_{1i} \cdot \sum_{i=1}^N K_{2i} \cdot \sum_{i=1}^N K_{3i}}{(10N)^3} \quad (2)$$

где K_{1i} , K_{2i} , K_{3i} – баллы, выставленные i -м экспертом трем указанным выше критериям соответственно.

Сами по себе угрозы не опасны для информационных систем. Сосуществуя совместно с ним, угрозы могут вовсе не причинять ущерба их безопасности. Опасность представляют только те угрозы, для которых информационная система является уязвимой, или, иными словами, обладает определенными уязвимостями, через которые источники угроз могут реализовать свои угрозы и нанести ущерб. Уязвимость информационной системы – это присущие ей причины, приводящие к нарушению безопасности ее функционирования или безопасности обрабатываемой в ней информации.

В качестве критериев оценки опасности уязвимости источник [10] предлагает: фатальность наличия у объекта информатизации уязвимости (K_4), доступность уязвимости для источников угроз (K_5), а также количество уязвимостей на объекте или частота их появления (K_6). Аналогично с процессом оценки опасности угроз один или N экспертов выставляют баллы от 1 до 10 по каждому из критериев. Для одного эксперта коэффициент опасности уязвимости вычисляется по схожей с (1) формулой:

$$K_{\text{опуз}} = \frac{K_4 K_5 K_6}{10^3} \quad (3)$$

Для N независимых экспертов расчет общего коэффициента опасности уязвимости производится аналогично формуле (2):

$$K_{\text{опузаВ}} = \frac{\sum_{i=1}^N K_{4i} \cdot \sum_{i=1}^N K_{5i} \cdot \sum_{i=1}^N K_{6i}}{(10N)^3} \quad (4)$$

При наличии множества уязвимостей информационной системы и множества угроз ее безопасности в реальных условиях функционирования велика вероятность реализации одной из угроз, нацеленной на процесс функционирования объекта или безопасность информации, которая в нем используется. Анализируя коэффициенты опасности совокупности уязвимостей, можно произвести их ранжирование и определить те из них, устранением которых необходимо заняться в первую очередь.

Для защиты информационных систем от атак разрабатываются специальные мероприятия по обеспечению их безопасности, часть из которых обеспечивает их надежное функционирование в условиях воздействия угроз, часть направлено на обеспечение информационной безопасности, т. е. сохранению таких свойств защищаемой информации, как конфиденциальность, доступность и целостность.

Учитывая многообразие угроз современного информационного мира, построить абсолютно адекватную систему защиты не представляется возможным, ведь затраты на ее организацию и сопровождение не должны превышать предполагаемый ущерб от ее нарушения в результате реализации угроз. Таким образом, необходимо выбрать методiku, которая позволит выбрать наиболее опасные для исследуемой информационной системы угрозы и защищаться только от них. Также важным является определение наиболее опасных уязвимостей, устранение которых позволит существенно повысить уровень безопасности информационной системы.

Существующие методы ранжирования угроз и уязвимостей производят их оценку независимо друг от друга [10]. Однако, как было указано выше, угрозы не представляют опасности для информационных систем без наличия соответствующих им уязвимостей. Также и уязвимости не подрывают уровень безопасности системы, если нет угроз, которые могут ими воспользоваться. Следовательно, оценку угроз и уязвимостей следует производить совокупно, оценивая критерии опасности

угрозы и уязвимости исходя из того, что первая будет реализована через вторую. При этом следует использовать подкорректированные критерии, соответствующие указанной совокупной оценке «угроза – уязвимость»:

– критерий С1 – возможность возникновения источника угрозы в достаточном окружении от информационной системы для реализации угрозы через уязвимость;

– критерий С2 – степень готовности источника угрозы воспользоваться уязвимостью информационной системы и реализовать угрозу;

– критерий С3 – распространенность уязвимости по информационной системе или частота ее появления;

– критерий С4 – доступность уязвимости для реализации угрозы ее источником;

– критерий С5 – фатальность от реализации угрозы источником угрозы через уязвимость информационной системы.

Все критерии оцениваются экспертами по десятибалльной шкале (дискретно от 1 до 10). Принцип выставления баллов для первых четырех критериев следующий: чем в большей степени появляется критерий, тем большего балла он заслуживает.

Критерии С1 и С2 в паре «угроза – уязвимость» в большей степени имеют отношение к угрозе, а критерии С3 и С4 – к уязвимости.

Критерий С5 в одинаковой степени зависит как от угрозы, так и от уязвимости, и для него целесообразно использовать более конкретизированную систему оценивания.

При оценке фатальности от реализации угрозы для объектов информатизации, важно не только принимать во внимание нарушение информационной безопасности, но также учитывать и функциональную безопасность. Ниже представлены баллы и соответствующие им уровни нарушения безопасности объектов информатизации исходя из соображений первостепенной важности обеспечения функциональной безопасности для объектов информатизации:

1 – нарушение доступности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

2 – нарушение конфиденциальности или целостности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

3 – нарушение конфиденциальности и целостности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

4 – нарушение конфиденциальности, целостности и доступности информации объекта информатизации, не приведшее к нарушению его функциональной безопасности;

5 – частичное нарушение функциональной безопасности объекта информатизации;

6 – нарушение доступности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

7 – нарушение конфиденциальности или целостности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

8 – нарушение конфиденциальности и целостности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

9 – нарушение конфиденциальности, целостности и доступности информации объекта информатизации, сопровождающееся частичным нарушением его функциональной безопасности;

10 – нарушение функциональной безопасности объекта информатизации – полный его выход из строя.

При таком подходе оценивается опасность реализации угрозы через уязвимость информационной системы. Общий коэффициент опасности реализации угрозы через уязвимость (КопугузN) оценивается N экспертами по следующей формуле:

$$K_{\text{опугузN}} = \frac{\sum_{i=1}^N C_{1i} \cdot \sum_{i=1}^N C_{2i} \cdot \sum_{i=1}^N C_{3i} \cdot \sum_{i=1}^N C_{4i} \cdot \sum_{i=1}^N C_{5i}}{(10N)^5} \quad (5)$$

В реальных условиях функционирования одна и та же уязвимость безопасности информационной системы может стать причиной реализации сразу нескольких угроз.

Для перекрестной оценки опасности угроз и уязвимостей в таких условиях необходимо учитывать все сочетания пар «угроза – уязвимость», для которых были проведены индивидуальные оценки по формуле (5).

Оценка опасности угрозы, которая может быть реализована через S уязвимостей, каждая из которых по отдельности была оценена группой из N экспертов по методике, указанной выше, рассчитывается следующим образом:

$$K_{\text{опугNS}} = \frac{\sum_{j=1}^S \sum_{i=1}^N C_{1ij} \cdot \sum_{j=1}^S \sum_{i=1}^N C_{2ij}}{(10NS)^2} \times \frac{\sum_{j=1}^S \sum_{i=1}^N C_{3ij} \cdot \sum_{j=1}^S \sum_{i=1}^N C_{4ij}}{(10N)^2} \cdot \frac{\max(\sum_{j=1..S} C_{5ij})}{10N}, \quad (6)$$

где C_{1ij}, C_{2ij}, C_{3ij}, C_{4ij}, C_{5ij} – баллы, выставленные i-м экспертом пяти указанным выше критериям соответственно в процессе оценки реализации одной угрозы через j-ю уязвимость информационной системы.

Схожим образом производится расчет коэффициента опасности уязвимости, через которую могут реализоваться Z угроз:

$$K_{\text{опуязNZ}} = \frac{\sum_{j=1}^Z \sum_{i=1}^N C_{1ij} \cdot \sum_{j=1}^Z \sum_{i=1}^N C_{2ij}}{(10N)^2} \times \frac{\sum_{j=1}^Z \sum_{i=1}^N C_{3ij} \cdot \sum_{j=1}^Z \sum_{i=1}^N C_{4ij}}{(10NZ)^2} \cdot \frac{\max(\sum_{i=1}^N C_{5ij})}{10N}, \quad (7)$$

где C_{1ij}, C_{2ij}, C_{3ij}, C_{4ij}, C_{5ij} – баллы, выставленные i-м экспертом пяти указанным выше критериям соответственно в процессе оценки одной уязвимости объекта информатизации при реализации через нее j-й угрозы.

Таким образом, при проведении перекрестной оценки угроз и уязвимостей необходимо:

- определить совокупности угроз и уязвимостей безопасности информационной системы;
- увязать между собой угрозы и уязвимости, установив потенциальную реализацию первых через вторые;
- перевести в резерв несвязанные уязвимости и угрозы;

– вычислить по формуле (5) коэффициент опасности реализации каждой угрозы через каждую уязвленную с ней уязвимость;

– для каждой из угроз и уязвимостей определить соответственно по формулам (6) и (7) коэффициенты их опасностей;

– произвести ранжирование угроз и уязвимостей, определив тем самым наиболее опасные из них.

Степень доступности к защищаемому объекту может быть классифицирована по следующей шкале:

– высокая степень доступности - антропогенный источник угроз имеет полный доступ к техническим и программным средствам обработки защищаемой информации (характерно для внутренних антропогенных источников, наделенных максимальными правами доступа, например, представители служб безопасности информации, администраторы);

– первая средняя степень доступности - антропогенный источник угроз имеет возможность опосредованного, не определенного функциональными обязанностями, (за счет побочных каналов утечки информации, использования возможности доступа к привилегированным рабочим местам) доступа к техническим и программным средствам обработки защищаемой информации (характерно для внутренних антропогенных источников);

– вторая средняя степень доступности - антропогенный источник угроз имеет ограниченную возможность доступа к программным средствам в силу введенных ограничений в использовании технических средств, функциональных обязанностей или по роду своей деятельности (характерно для внутренних антропогенных источников с обычными правами доступа, например, пользователи, или внешних антропогенных источников, имеющих право доступа к средствам обработки и передачи защищаемой информации, например, хакеры, технический персонал поставщиков телематических услуг);

– низкая степень доступности - антропогенный источник угроз имеет очень ограниченную возможность доступа к техническим средствам и программам, обрабатывающим

защищаемую информацию (характерно для внешних антропогенных источников).

– отсутствие доступности - антропогенный источник угроз не имеет доступа к техническим средствам и программам, обрабатывающих защищаемую информацию.

Степень удаленности от защищаемого объекта можно характеризовать следующими параметрами:

– совпадающие объекты - объекты защиты сами содержат источники техногенных угроз и их территориальное разделение невозможно;

– близко расположенные объекты - объекты защиты расположены в непосредственной близости от источников техногенных угроз и любое проявление таких угроз может оказать существенное влияние на защищаемый объект;

– средне удаленные объекты - объекты защиты располагаются на удалении от источников техногенных угроз, на котором проявление влияния этих угроз может оказать не существенное влияние на объект защиты;

– удаленно расположенные объекты - объект защиты располагается на удалении от источника техногенных угроз, исключая возможность его прямого воздействия.

– сильно удаленные объекты - объект защиты располагается на значительном удалении от источников техногенных угроз, полностью исключая любые воздействия на защищаемый объект, в том числе и по вторичным проявлениям.

Особенности обстановки характеризуются расположением объектов защиты в различных природных, климатических, сейсмологических, гидрологических и других условиях. Особенности обстановки можно оценить по следующей шкале:

– очень опасные условия - объект защиты расположен в зоне действия природных катаклизмов;

– опасные условия - объект защиты расположен в зоне, в которой многолетние наблюдения показывают возможность проявления природных катаклизмов;

– умеренно опасные условия - объект защиты расположен в зоне в которой по проводимым наблюдениям на протяжении долгого периода отсутствуют проявления природных

катаклизмов, но имеются предпосылки возникновения стихийных источников угроз на самом объекте;

– слабо опасные условия - объект защиты находится вне пределов зоны действия природных катаклизмов, однако на объекте имеются предпосылки возникновения стихийных источников угроз;

– неопасные условия - объект защиты находится вне пределов зоны действия природных катаклизмов и на объекте отсутствуют предпосылки возникновения стихийных источников угроз.

2.2 Системы обнаружения и предотвращения атак

Система обнаружения атак - программное или аппаратное средство, предназначенное для выявления фактов неавторизованного доступа в компьютерную систему или сеть либо несанкционированного управления ими в основном через Интернет. Соответствующий английский термин — Intrusion Detection System (IDS). Системы обнаружения вторжений обеспечивают дополнительный уровень защиты компьютерных систем.

Системы обнаружения атак используются для обнаружения некоторых типов вредоносной активности, которая может нарушить безопасность компьютерной системы. К такой активности относятся сетевые атаки против уязвимых сервисов, атаки, направленные на повышение привилегий, неавторизованный доступ к важным файлам, а также действия вредоносного программного обеспечения (компьютерных вирусов, троянов и червей). Обычно архитектура систем обнаружения атак включает:

– сенсорную подсистему, предназначенную для сбора событий, связанных с безопасностью защищаемой системы;

– подсистему анализа, предназначенную для выявления атак и подозрительных действий на основе данных сенсоров;

– хранилище, обеспечивающее накопление первичных событий и результатов анализа;

– консоль управления, позволяющая наблюдать за состоянием защищаемой системы и системы обнаружения атак, просматривать выявленные подсистемой анализа инциденты.

Существует несколько способов классификации системы обнаружения атак в зависимости от типа и расположения сенсоров, а также методов, используемых подсистемой анализа для выявления подозрительной активности. Во многих простых системах обнаружения атак все компоненты реализованы в виде одного модуля или устройства

Системы предотвращения атак (Intrusion Prevention Systems или сокращенно IPS) являются развитием систем обнаружения атак (Intrusion Detection Systems или сокращенно IDS). Но если IDS лишь детектировали угрозы в сети и на хостах, посылали администратору оповещения различными способами, то IPS сейчас блокируют атаки сразу в момент их появления. Кроме того, IPS интегрируются с другими средствами защиты: межсетевыми экранами, сканерами безопасности, системами управления инцидентами и даже антивирусами. Для каждой атаки сейчас есть возможность провести полный анализ инцидента: собрать пакеты, идущие от атакующего, инициировать расследование, произвести устранение уязвимости. В итоге системой управления производится контроль самого администратора сети, который должен не только устранить уязвимость, например поставив патч, но и отчитаться перед системой о проделанной работе.

Одной из характеристик, по которой можно оценивать IPS является величина задержек в сети, которые неизбежно вносят такие системы.

Как правило, эту информацию можно взять у самого производителя или из исследований независимых тестовых лабораторий, например NSS.

Второй такой характеристикой является количество ложных срабатываний. Администратор рано или поздно перестанет обращать на постоянные ложные срабатывания, из-за чего может пропустить действительно важное оповещение. В некоторых IDS встроены методы корреляции, которые упорядочивают найденные атаки по уровню критичности, пользуясь информацией из других источников, например из сканера безопасности. Если он увидел, что на компьютере стоит SUN

Boluris и Oracle, то можно со 100%-ной уверенностью сказать, что атака червя Slammer (которая нацелена на Microsoft SQL Server) на данный сервер не пройдет. Таким образом, системы корреляции помечают часть атак неудавшимися, что сильно облегчает работу администратора.

Третьей характеристикой являются методы обнаружения/блокирования атак и возможность их тюнинга под требования своей сети. Тут появляется такое понятие, как «превентивная защита», – возможность защиты от атак, которые еще неизвестны. Такие технологии уже есть, и их надо использовать. Тут, к сожалению, нужно отметить, что еще нет систем, которые бы одновременно использовали два известных метода анализа атак: анализ протоколов (или сигнатурный) и поведенческий. Поэтому для полноценной защиты придется установить в сети минимум два устройства. Одно будет использовать алгоритмы поиска уязвимостей при помощи сигнатур и анализа протоколов, другое – статистические и аналитические методы по анализу аномалий в поведении сетевых потоков. Сигнатурные методы используются во многих системах обнаружения и предотвращения атак, но, к сожалению, не оправдывают себя: они не обеспечивают превентивной защиты, поскольку для выпуска сигнатуры требуется наличие эксплойта. Поэтому самыми передовыми методами анализа атак сейчас является полный анализ протокола, когда не анализируется конкретная атака, а ищется в протоколе признак использования атакующим уязвимости. Если перед проведением атаки необходимо установление соединения, то система по анализу протоколов проверит, прошло ли оно успешно или его не было. А сигнатурная система выдаст ложное срабатывание, поскольку у нее нет такого функционала.

Поведенческие системы работают совершенно по-другому. Они анализируют сетевой трафик и запоминают, какие обычно идут сетевые потоки. Как только возникает трафик, который не соответствует запомненному поведению, становится ясно, что в сети что-то происходит новое: например, распространение червя. Кроме того, такие системы связаны с центром обновлений и раз в час получают новые правила поведения червей и другие обновления. Например, списки фишинговых сайтов, что позволяет сразу их блокировать, и т.п. Для провайдеров такие

системы важны тем, что они позволяют отслеживать изменения в "грузопотоке". Провайдеру важно обеспечить скорость и надежность доставки пакетов, а для хозяина небольшой сети необходимо, чтобы внутри нее не завелись атакующие, чтобы сеть не записали в черный список спамеров и чтобы атакующие не забили весь канал в Интернете мусором.

2.3 Сканеры безопасности

Сканеры безопасности – это программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющее сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости.

Сканеры безопасности позволяют проверить различные приложения в системе на предмет наличия «дыр», которыми могут воспользоваться злоумышленники. Также могут быть использованы низкоуровневые средства, такие как сканер портов, для выявления и анализа возможных приложений и протоколов, выполняющихся в системе.

Работу сканера уязвимостей можно разбить на 4 шага:

1 Обычно, сканер сначала обнаруживает активные IP-адреса, открытые порты, запущенную операционную систему и приложения;

2 Составляется отчет о безопасности (необязательный шаг);

3 Попытка определить уровень возможного вмешательства в операционную систему или приложения (может повлечь сбой);

4 На заключительном этапе сканер может воспользоваться уязвимостью, вызвав сбой операционной системы или приложения.

Сканеры могут быть вредоносными или «дружественными». Последние обычно останавливаются в своих действиях на шаге 2 или 3, но никогда не доходят до шага 4.

Среди сканеров безопасности можно выделить:

- сканер портов;
- сканеры, исследующие топологию компьютерной сети;
- сканеры, исследующие уязвимости сетевых сервисов;
- сетевые черви;

– CGI-сканеры («дружественные» – помогают найти уязвимые скрипты).

Одним из важнейших этапов обеспечения информационной безопасности является идентификация потенциальных рисков. Большинство ИТ-специалистов знают, насколько может быть опасна «брешь» в ОС и приложениях. И чрезвычайно важно найти эти «дыры», или на языке профессионалов – уязвимости, прежде, чем ими смогут воспользоваться недоброжелатели. Для этой цели и были созданы сканеры безопасности.

Продвинутые специалисты по IT-безопасности используют в своей работе специализированное аппаратное или программное обеспечение, сканирующее сеть и ее устройства на предмет обнаружения слабых мест в системе безопасности. Это и есть сканеры уязвимости, или по-другому – безопасности, сети. Они проверяют используемые приложения, ищут «дыры», которыми могли бы воспользоваться хакеры, и предупреждают администратора о зонах риска системы. Грамотно используя сканер уязвимости сети, специалист может значительно усилить сетевую безопасность. Таким образом, сетевые сканеры направлены на решение следующих задач:

- идентификация и анализ уязвимостей;
- инвентаризация ресурсов, таких как операционная система, программное обеспечение и устройства сети;
- формирование отчетов, содержащих описание уязвимостей и варианты их устранения.

Сканер локальной сети – жизненно необходимое средство для компаний, чья деятельность напрямую связана с хранением и обработкой уникальных баз данных, конфиденциальной информации, ценных архивов. Без сомнения, сканеры сети необходимы организациям в сферах обороны, науки, медицины, торговли, IT, финансов, рекламы, производства, для органов власти и диспетчерских служб — словом, везде, где нежелательна или даже опасна утечка накопленной информации, имеются базы персональных данных клиентов.

Сканеры локальной сети при своей работе используют два основных механизма:

1) Первый – зондирование – не слишком оперативен, но точен. Это механизм активного анализа, который запускает имитации атак, тем самым проверяя уязвимость. При

зондировании применяются методы реализации атак, которые помогают подтвердить наличие уязвимости и обнаружить ранее не выявленные «провалы».

2) Второй механизм – сканирование – более быстрый, но дает менее точные результаты. Это пассивный анализ, при котором сканер ищет уязвимость без подтверждения ее наличия, используя косвенные признаки. С помощью сканирования определяются открытые порты и собираются связанные с ними заголовки. Они в дальнейшем сравниваются с таблицей правил определения сетевых устройств, ОС и возможных «дыр».

После сравнения сетевой сканер безопасности сообщает о наличии или отсутствии уязвимости. В общем случае алгоритм работы сканеров следующий:

- проверка заголовков. Самый простой и быстрый способ на основе сканирования, однако имеющий ряд недостатков. Так, вывод о «провале» делается лишь по результатам анализа заголовков. К примеру, проверяя FTP-сервер, сканер узнает версию обеспечения и на основе этой информации сообщает о возможных уязвимостях. Естественно, специалисты по сетевой безопасности осведомлены о ненадежности этого метода, однако как первый шаг сканирования – это оптимальное решение, не приводящее к нарушению работы сети;

- активные зондирующие проверки. Это сканирование, при котором не проверяется версия ПО, а сравнивается «цифровой слепок» фрагмента программы со «слепком» уязвимости. По тому же принципу действуют антивирусные программы, сравнивая ПО с имеющимися в базе сигнатурами вирусов. Тоже достаточно быстрый метод, хотя и медленнее первого, с большим коэффициентом надежности;

- имитация атак. Это зондирование, которое эксплуатирует дефекты в программном обеспечении. Таким образом подается своеобразный импульс некоторым уязвимостям, которые не заметны до определенного момента. Эффективный метод, однако применить его можно не всегда. Так, вероятно ситуация, когда даже имитируемая атака просто отключит проверяемый узел сети.

Большинство современных сканеров безопасности сети работает по нижеперечисленным принципам:

- сбор информации о сети, идентификация всех активных устройств и сервисов, запущенных на них;
- обнаружение потенциальных уязвимостей;
- подтверждение выбранных уязвимостей, для чего используются специфические методы и моделируются атаки; формирование отчетов;
- автоматическое устранение уязвимостей. Не всегда данный этап реализуется в сетевых сканерах безопасности, но часто встречается в сканерах системных. Существует возможность создания резервного сценария, который может отменить произведенные изменения, – например, если после устранения уязвимости будет нарушено полноценное функционирование сети.

Вопросы для самоконтроля:

- 1 Что из себя представляют системы обнаружения атак?
- 2 Из чего состоит архитектура систем обнаружения атак?
- 3 В чём отличие системы предотвращения атак от систем обнаружения атак?
- 4 По каким характеристикам можно оценивать IPS?
- 5 Понятие сканера безопасности. Принцип работы.
- 6 Классификация сканеров безопасности.
- 7 Понятие и классификация уязвимостей.
- 8 Понятие и классификация угроз.
- 9 Понятие и классификация атак.
- 10 Принципы методики вычисления коэффициента опасности (КО)?

3 ПРАКТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ ПРОГРАММЫ CRYPTOOOL2

3.1 Освоение метода шифрования и дешифрования по алгоритму Цезаря в среде CryptTool2

Шифр Цезаря относится к симметричным шифрам подстановки, когда каждый символ в открытом тексте заменяется буквой, находящейся на некотором постоянном числе позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3 буква «А» будет заменена на букву «Г», «Б» станет «Д», и так далее (рисунок 3.1).

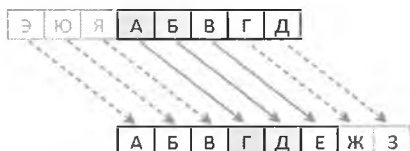


Рисунок 3.1 – Шифр Цезаря

Для декодирования данного шифра достаточно знать значение сдвига, либо методом подбора выявить этот сдвиг.

Среда CryptTool 2 – это набор инструментов для кодирования и декодирования библиотек и компонентов, включая классические (симметричные) и современные (асимметричные) алгоритмы.

Все шифры и дополнительные устройства, используемые в программе, сделаны в виде функционал блоков. Имеющие модуль настройки определенных соответствующих ей параметров для этого CryptTool 2 предоставляет графический пользовательский интерфейс для визуального программирования. Тот же компонент может визуализировать свои внутренние операции. Это делает его удобным для пользователя, чтобы он мог проследить все детали криптографического алгоритма и увидеть более широкую картину того, какой сценарий использует этот шифр или блок в реальной жизни.

Функциональные блоки имеют модули для ввода и вывода информации в процессе работы, которые в свою очередь могут присоединяться к другим функциональным блокам и обмениваться информацией между собой. Каждый блок имеет сценарий работы и виртуализации. Это дает возможность после сборки всей схемы запустить симуляцию работы. После запуска симуляции каждый из блоков начинает постепенную загрузку с отображением процесса в виде процентного выполнения. По окончании на каждом блоке и а также в отчетном окне отображается полный ход действий, в котором могут отображаться ошибки и нестыковки блоков ввиду передаваемой информации. Это облегчает работу преподавателя и позволяет пользователю самостоятельно разобраться в ошибке. Также пользователь прослеживает в процессе симуляции все данные на входе выходе каждого блока простым наведением курсора.

3.1.1 Построение схемы Шифра Цезаря в среде CrypTool2.

Открыть программу CrypTool2: Пуск – Программы – CrypTool2.

Создать новый проект: Home – New – Workspace (Главная – Новый – Рабочее пространство) (рисунок 3.2).



Рисунок 3.2 – Создание нового проекта

Вытащить на рабочее пространство блок, отвечающий за шифр Цезаря (рисунок 3.3): Classic Ciphers – Caesar (Классические шифры – Цезарь).

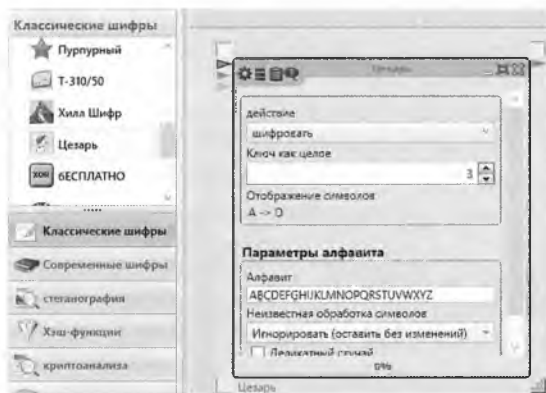


Рисунок 3 – Блок шифра Цезаря

Добавить блоки ввода-вывода текста: Инструменты – Ввод текста – Вывод текста (Tools – Input text – Output text).

Соединить блоки между собой как показано на рисунке 3.4:

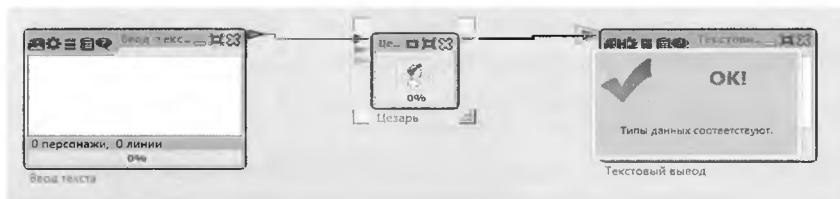


Рисунок 3.4 – Схема шифра Цезаря


Из таблицы 3.1 выбрать, согласно варианта, исходное сообщение для шифрования и ключ шифрования.

Таблица 3.1 – Исходные данные для шифрования

Вариант	Сообщение	Ключ
1	The difficulty of solving classical ciphers varies between very easy and very hard. For example, monoalphabetic substitution ciphers can be solved easily by hand.	3
2	More complex ciphers like the polyalphabetic Vigenere cipher, are harder to solve ` and the solution by hand takes much more time. Machine ciphers like the Enigma rotor machine, are nearly impossible to be solved only by hand.	5

3	To support researchers, cryptanalysts, and historians analyzing ciphers, the open-source software CryptTool 2 was implemented.	7
4	It contains a broad set of tools and methods to automate the cryptanalysis of different (classical and modern) ciphers. In this paper, we present a step-by-step approach for analyzing classical ciphers and breaking these with the help of the tools in CT2.	6
5	There are several historical documents containing text enciphered with different encryption algorithms. Such books can be found for instance in the secret archives of the Vatican. Often, historians who find such encrypted books during their research are not able to decipher and reveal the plaintext.	5
6	Many encrypted historical books that survived history are available. Most of them are encrypted either with simple monoalphabetic substitutions or with homophone substitutions. For some books the type of cipher is unknown.	4
7	Many encrypted historical messages are encrypted with simple substitution ciphers, homophone substitution ciphers, polyalphabetic substitution ciphers, nomenclatures, or codebooks.	8
8	Homophone substitutions as well as polyalphabetic substitutions flatten the distribution of letters, hence, aiming to destroy the possibility to break the cipher with statistics. Nevertheless, having enough ciphertext and using sophisticated algorithms, e.g. hill climbing and simulated annealing, it is still possible to break them.	9
9	For breaking a classical cipher, it is useful to know the language of the plaintext. It is possible to break a cipher using a “wrong” language, but the correct one yields a higher chance of success. For cryptanalysis most of the algorithms implemented in CT2 contain a set of multiple languages.	10
10	The WorkspaceManager is the heart of CT2 since it enables the user to create arbitrary cascades of ciphers and cryptanalysis methods using graphical icons (components) that can be connected. To create a cascade, the user may drag&drop components (ciphers, analysis methods, and tools) onto the so-called workspace.	15
11	The Startcenter is the first screen appearing when CT2 starts. From here, a user can come to every other component by just clicking an icon.	7

12	The Wizard is intended for CT2 users that are not yet very familiar with the topics cryptography or cryptanalysis. The user just selects step by step what he wants to do. The wizard displays at each step a small set of choices for the user	11
13	With the Vigenere cipher for example, it would change the first letter of the keyword. After changing the letter, it again computes the cost function. If the result is higher than for the previous key, the new key is accepted. Otherwise, the new key is discarded and another modified one is tested	5
14	The algorithm performs these steps until no new modified key can be found that yields a higher cost value, i.e. the hill (local maximum) of the fitness score is reached. Most of our classical cryptanalytic implementations in CT2 are based on such a hill climbing approach.	13
15	CrypTool 2 (CT2) is an open-source tool for elearning cryptology. The CrypTool community aims to integrate into CT2 the best known and most powerful algorithms to automatically break (classical and modern) ciphers. Additionally, our goal is to make CT2 a tool that can be used by everyone who needs to break a classical cipher.	6

Запуск схемы осуществляется кнопкой  Играть, остановка -



Для дешифрования можно добавить еще один блок шифра Цезаря, в котором в параметрах установить пункт «расшифровать» и блок вывода текста (рисунок 3.5).

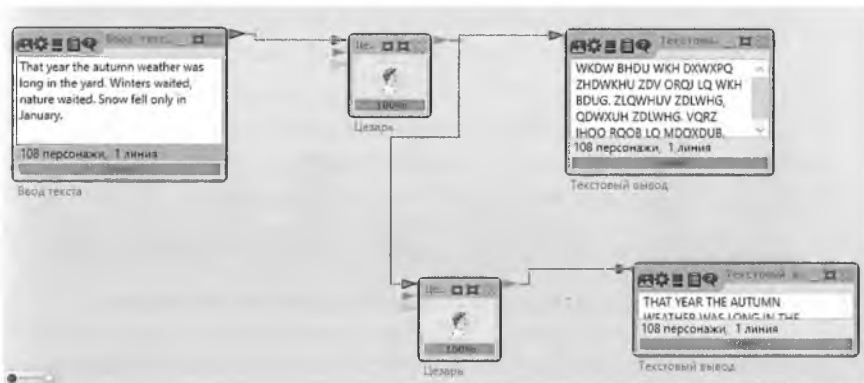


Рисунок 3.5 – Схема шифрования/дешифрования

3.1.2 Частотный анализ.

Добавить из вкладки «Криптоанализ» следующие блоки для частотного анализа: частотный текст – анализатор Цезарь. А так же блок шифра Цезаря и для вывода текста (рисунок 3.6).

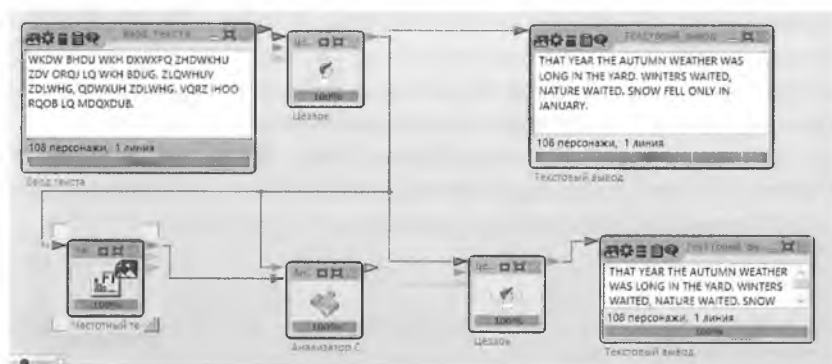


Рисунок 3.6 – Схема частотного анализа

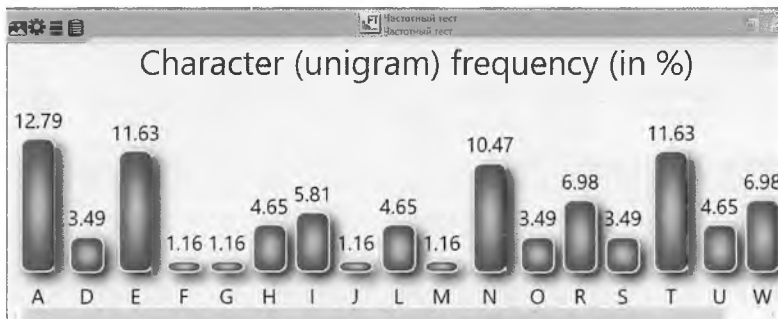


Рисунок 3.7 – Результат частотного анализа шифра Цезаря

3.1.3 Взлом шифра Цезаря с помощью Brute Force.

Собрать схему шифра Цезаря с учетом Brute Force, добавив блок ввода текста для подбора значения Brute Force и конвертер.

Установить в настройках конвертера преобразование в тип «ИНТ», порядок байтов – большой Эндриан. В блоке шифра Цезаря настроить дешифрование.

Соединить сначала!!! блок ввода значения Brute Force с конвертером и блоком шифра Цезаря, а также блока вывода текста. Запустить работу схемы для загрузки. После чего остановить схему и соединить ее с входным блоком, в котором будет содержаться зашифрованное сообщение.

Заново запустить схему через «Play» и начать подбирать значение ключа. Когда значение будет верно, в блоке вывода текста появится понятный исходный текст сообщения.

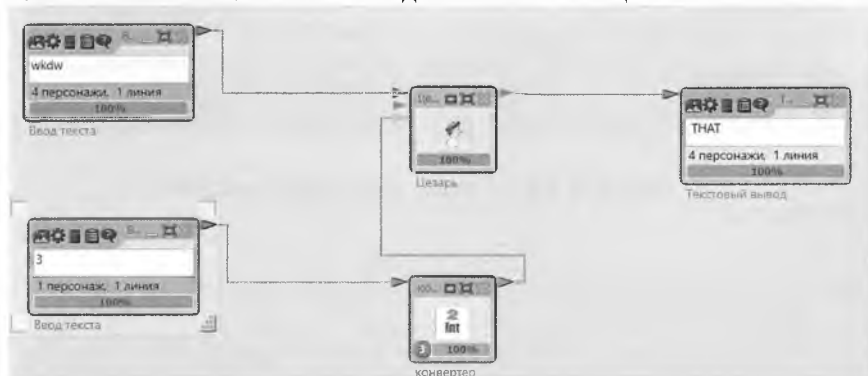


Рисунок 3.8 – Окно реализации атаки на шифр Цезаря

3.2 Исследование и криптоанализ алгоритма RSA

Алгоритм RSA был разработан в 1977 году Рональдом Ривестом, Ади Шамиром и Леном Адлеманом и опубликован в 1978 году. С тех пор алгоритм Rivest-Shamir-Adleman (RSA) широко применяется практически во всех приложениях, использующих криптографию с открытым ключом [1, 2, 3].

Наиболее перспективными системами криптографической защиты данных являются системы с открытым ключом. В таких системах для зашифрования данных используется один ключ, а для расшифрования другой. Первый ключ не является секретным и может быть опубликован для использования всеми пользователями системы, которые зашифровывают данные. Расшифрование данных с помощью известного ключа невозможно. Для расшифрования данных получатель зашифрованной информации использует второй ключ, который является секретным. Разумеется, ключ расшифрования не может быть определен из ключа зашифрования.

Для исследования алгоритма RSA определим его суть. RSA – криптографическая система открытого ключа, обеспечивающая такие механизмы защиты как шифрование и цифровая подпись (аутентификация – установление подлинности).

Алгоритм RSA работает следующим образом: берутся два достаточно больших простых числа p и q и вычисляется их произведение $n = p \cdot q$; n называется модулем.

Затем выбирается число e , удовлетворяющее следующему условию:

$$1 < e < (p - 1) \cdot (q - 1) \quad (3.1)$$

и не имеющее общих делителей кроме 1 с функцией Эйлера $(p - 1) \cdot (q - 1)$.

Затем вычисляется число d таким образом, что $(e \cdot d - 1)$ делится на число $(p - 1) \cdot (q - 1)$.

Где e – открытый (public) показатель;

d – частный (private) показатель;

$(n; e)$ – открытый (public) ключ;

$(n; d)$ – частный (private) ключ.

Делители (факторы) p и q можно либо уничтожить, либо сохранить вместе с частным (private) ключом.

Если бы существовали эффективные методы разложения на сомножители, то, разложив n на сомножители p и q , можно было бы получить частный ключ d . Таким образом, надежность криптосистемы RSA основана на трудноразрешимой – практически неразрешимой – задаче разложения n на сомножители, так как в настоящее время эффективного способа поиска сомножителей не существует.

Опишем алгоритм шифрования и дешифрования в системе Cryptool 2 Beta с помощью блоков, представленных на рисунке 3.9 и 3.10.

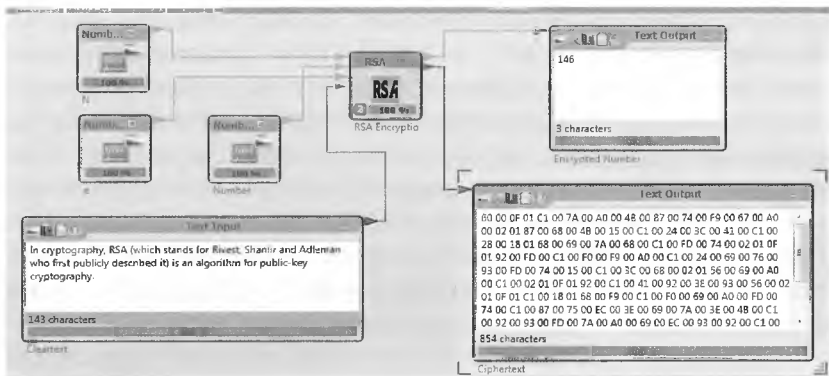


Рисунок 3.9 – Схема шифрования алгоритма RSA

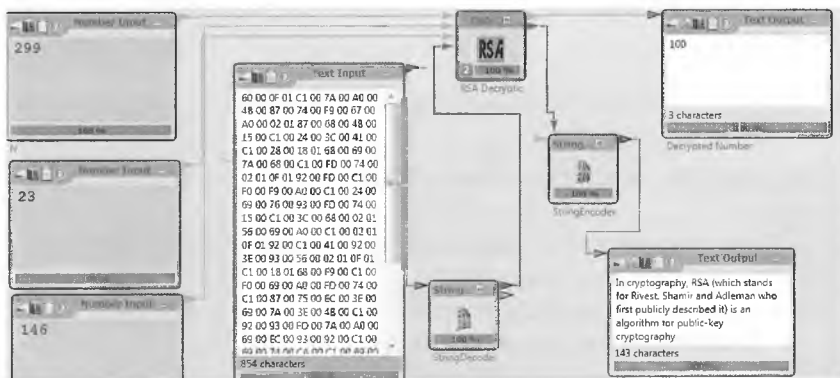


Рисунок 3.10 – Схема дешифрования алгоритма RSA

Существует несколько способов взлома RSA. Наиболее эффективная атака – найти секретный ключ, соответствующий необходимому открытому ключу. Это позволит нападающему читать все сообщения, зашифрованные открытым ключом, и подделывать подписи. Такую атаку можно провести, найдя главные сомножители (факторы) общего модуля $n = p$ и q . На основании p , q и e (общий показатель) нападающий может легко вычислить частный показатель d . Основная сложность в поиске главных сомножителей (факторинг) n . Безопасность RSA зависит от разложения на сомножители (факторинга), что является трудной задачей, не имеющей эффективных способов решения [2].

Фактически, задача восстановления секретного ключа эквивалентна задаче разложения на множители (факторинга) модуля: можно использовать d для поиска сомножителей n , и наоборот, можно использовать n для поиска d . Надо отметить, что усовершенствование вычислительного оборудования само по себе не уменьшит стойкость криптосистемы RSA, если ключи будут иметь достаточную длину. Фактически же совершенствование оборудования увеличивает стойкость криптосистемы.

Криптосистема RSA используется в самых различных продуктах, на различных платформах и во многих отраслях [3]. В настоящее время криптосистема RSA встраивается во многие коммерческие продукты, число которых постоянно увеличивается. Также ее используют операционные системы Microsoft, Apple, Sun и Novell. В аппаратном исполнении RSA алгоритм применяется в защищенных телефонах, на сетевых платах Ethernet, на смарт-картах, широко используется в криптографическом оборудовании. Кроме того, алгоритм входит в состав всех основных протоколов для защищенных коммуникаций Internet, в том числе S/MIME, SSL и S/WAN, а также используется во многих учреждениях, например, в правительственных службах, в большинстве корпораций, в государственных лабораториях и университетах. На осень 2000 года технологии с применением алгоритма RSA были лицензированы более чем 700 компаниями.

Технологию шифрования RSA BSAFE используют около 500 миллионов пользователей всего мира. Так как в большинстве случаев при этом используется алгоритм RSA, то его можно считать наиболее распространенной криптосистемой общего (public) ключа в мире и это количество имеет явную тенденцию к увеличению по мере роста Internet.

Распространение системы RSA дошло до такой степени, что ее учитывают при создании новых стандартов. При разработке стандартов цифровых подписей, в первую очередь в 1997 был разработан стандарт ANSI X9.30, поддерживающий Digital Signature Standard (стандарт Цифровой подписи). Годом позже был введен ANSI X9.31, в котором сделан акцент на цифровых подписях RSA, что отвечает фактически сложившейся ситуации в частности для финансовых учреждений.

Недостатки защищенной аутентификации (установления подлинности) были главным препятствием для замены бумажного документооборота электронным; почти везде контракты, чеки, официальные письма, юридические документы все еще выполняются на бумаге. Именно это – необходимость элементов бумажного документооборота – не позволяло полностью перейти к электронным транзакциям. Предлагаемая RSA цифровая подпись – инструмент, который позволит перевести наиболее существенные бумажные документо-потоки в электронно-цифровой вид. Благодаря цифровым подписям многие документы – паспорта, избирательные бюллетени, завещания, договора аренды – теперь могут существовать в электронной форме, а любая бумажная версия будет в этом случае только копией электронного оригинала. Все это стало возможным благодаря стандарту цифровых подписей RSA.

3.3 Реализация режимов шифрования алгоритма AES

Advanced Encryption Standard (AES) представляет собой блочный шифр, кодирующий 128-битный текстовый блок в 128-битный зашифрованный блок, или дешифрует 128-битный зашифрованный блок в 128-битный текстовый блок. AES-128, AES-192, AES-256 обрабатывают блоки данных за соответственно 10, 12 или 14 раундов. Каждый раунд представляет собой определенную последовательность трансформаций. Каждый

раунд работает с двумя 128-битными блоками: «текущий» и «ключ раунда». Все раунды используют разные «ключи раунда», которые получаются с помощью алгоритма расширения ключа. Этот алгоритм не зависит от шифруемых данных и может выполняться независимо от фазы шифрования/дешифрования.

3.3.1 Режим ECB.

Electronic Codebook (ECB) – это режим электронной кодовой книги (режим простой замены).

Для режима ECB справедлива схема, представленная на рисунке 3.11. То есть для применения данного режима к алгоритму AES и реализации в среде Cryptool 2 достаточно указать этот режим в настройках блока AES и подать на вход блока сообщение и ключ.

Однако в данной работе режим ECB будет реализован двумя способами:

1) AES будет работать в 128-битном режиме (то есть сообщение будет разделено на шифруемые блоки по 128 бит каждый), при этом ключ и сообщение будут отдельно друг от друга, а если введен ключ, в котором больше 16 символов, лишние символы будут отсекаются.

2) AES будет работать в 256-битном режиме (то есть сообщение будет разделено на шифруемые блоки по 256 бит каждый), при этом само шифруемое сообщение будет выступать в качестве ключа, а разделение на 256-битные блоки будет производиться вручную.



Рисунок 3.11 – Режим ECB

Реализация первой схемы показана на рисунке 3.12 с настройкой блока шифрования.



Рисунок 3.12 – Блок шифрования AES

Для реализации режима ECB нужно подать ключ (т.к алгоритм AES – симметричный алгоритм, значит для шифрования и для дешифрования нужен один и тот же ключ). Реализация данного режима (шифрование) первым способом представлена на рисунке 3.13.

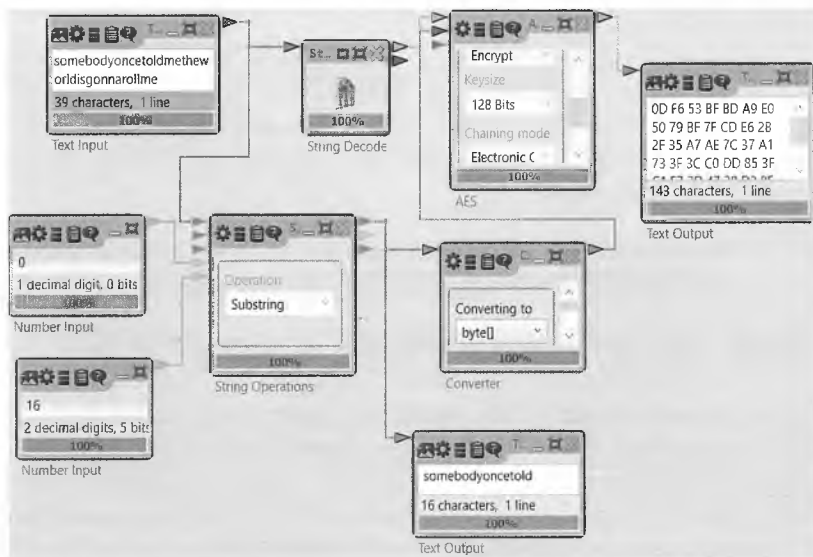


Рисунок 3.13 – Реализация шифрования в режима ECB

Пояснение этапов создания схемы:

1) Блок ввода текста пропускаем через String Decoder и подаем на вход как зашифрованное сообщение;

2) Подаем этот же блок на вход операции Substring(), которая возвращает подстроку из оригинальной строки. В качестве параметров выбора подстроки вводим 0 и 16, то есть нам нужно взять из оригинальной строки 16 символов, начиная с нулевого символа.

3) Далее извлеченную 16-символьную (128-битную) подстроку конвертируем в байтовый массив (Converter) и полученное значение подаем на вход ключа.

На рисунке 3.14 представлена полная схема: и шифрование, и дешифрование.

В данной схеме добавлен блок дешифрования, а на вход поданы зашифрованное сообщение и тот же ключ шифрования.

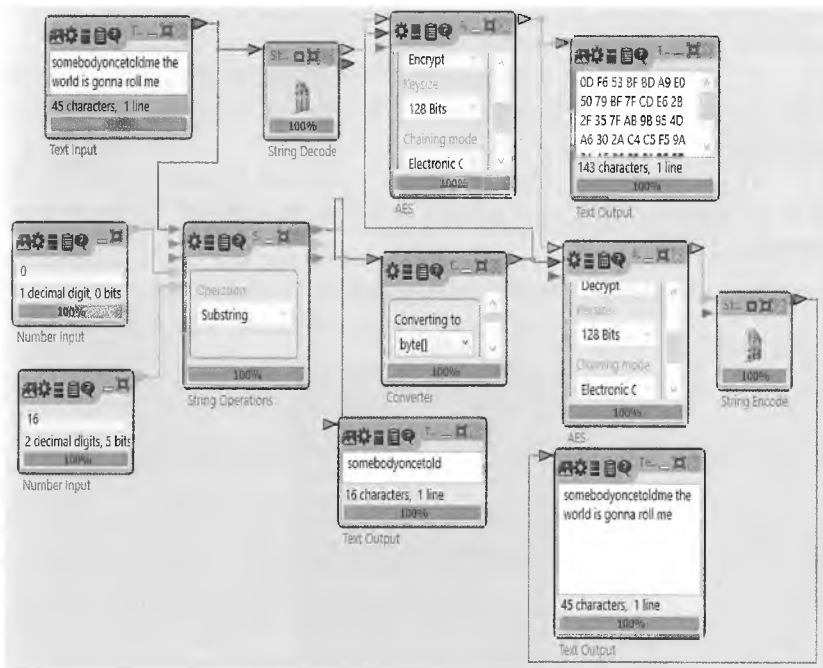


Рисунок 3.14 – Реализация шифрования и дешифрования в режиме ECB

Как уже упоминалось, в данном способе реализации AES будет работать в 256-битном режиме (то есть сообщение будет разделено на шифруемые блоки по 256 бит каждый), при этом само шифруемое сообщение будет выступать в качестве ключа, а разделение на 256-битные блоки будет производиться вручную.

Для этого сначала реализуем разделение сообщения на блоки по 32 символа (рисунок 3.15). Обратите внимание, что в сообщении 92 символа, и в данном способе схема будет работать без ошибок только для сообщения размером в 92 символа. Для сообщения другого размера ее необходимо будет изменить. Поясним работу части схемы, представленной на рисунке 3.15:

1) В Сообщение из `TextInput` подаем на вход трех блоков строковой операции `Substr()`, для разделения данной строки на 3 подстроки.

2) В качестве числовых параметров к первому блоку `String Operations` подаем 0 и 32, то есть указываем, что нам нужно извлечь из строки 32 символа, начиная с нулевого.

3) Ко второму блоку `String Operations` подаем 32 и 32, то есть указываем, что нам нужно извлечь из строки 32 символа, начиная с 32-го.

4) К третьему блоку `String Operations` подаем 64 и 28, то есть указываем, что нам нужно извлечь из строки 28 символов, начиная с 28-го.

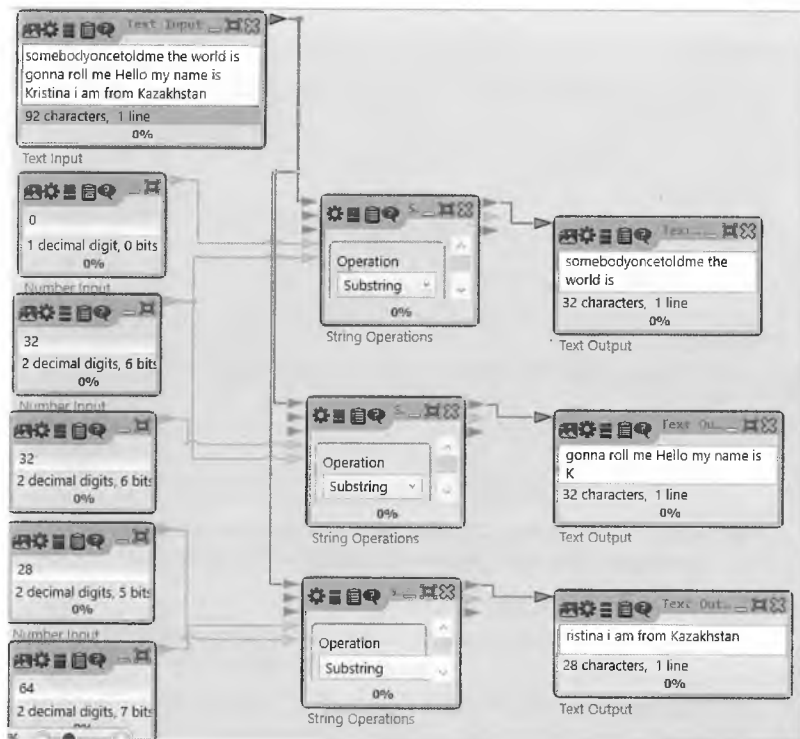


Рисунок 3.15 – Часть схемы, отвечающая за разделение сообщения

Для реализации шифрования будет добавлен блок с настройками, как показано на рисунке 3.16.



Рисунок 3.16 – Настройки блока AES

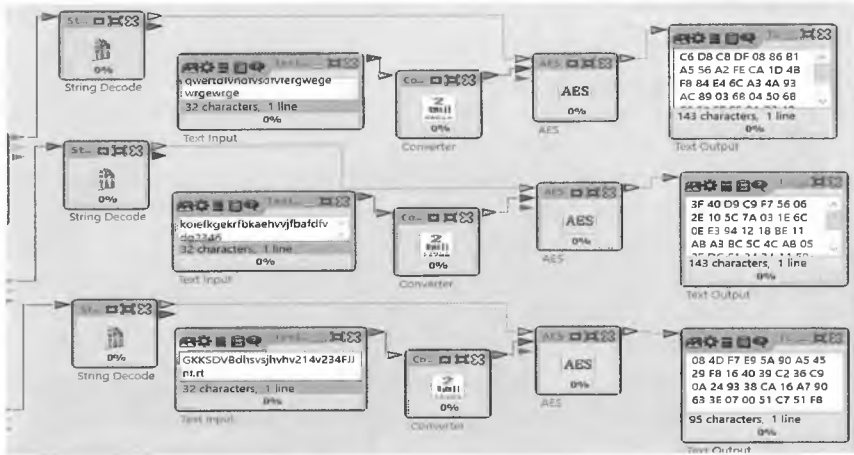


Рисунок 3.17 – Часть схемы, отвечающая за шифрование

Поясним часть схемы на рисунке 3.17:

- 1) 3 входных блока с разделенным сообщением прогоняем через String Decoder.
- 2) Формируем отдельный ключ для каждого из блоков и конвертируем каждый из них в байтовый массив.
- 3) Шифруем отдельно каждый блок и выводим результат.

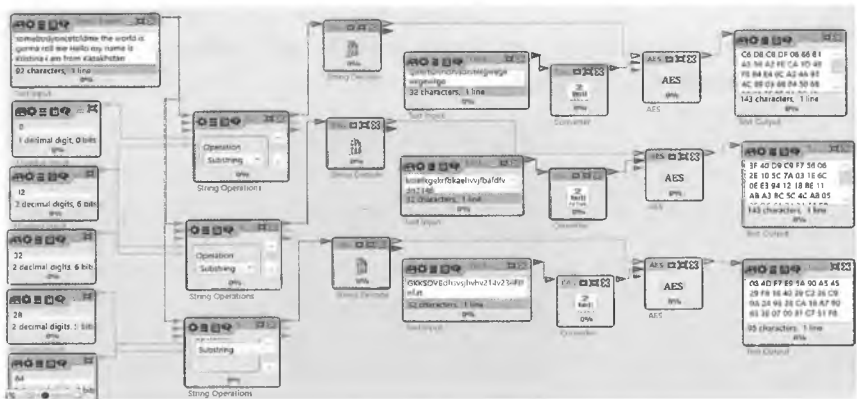


Рисунок 3.18 – Общая схема шифрования. Далее – часть схемы с дешифрованием (рисунок 3.19).

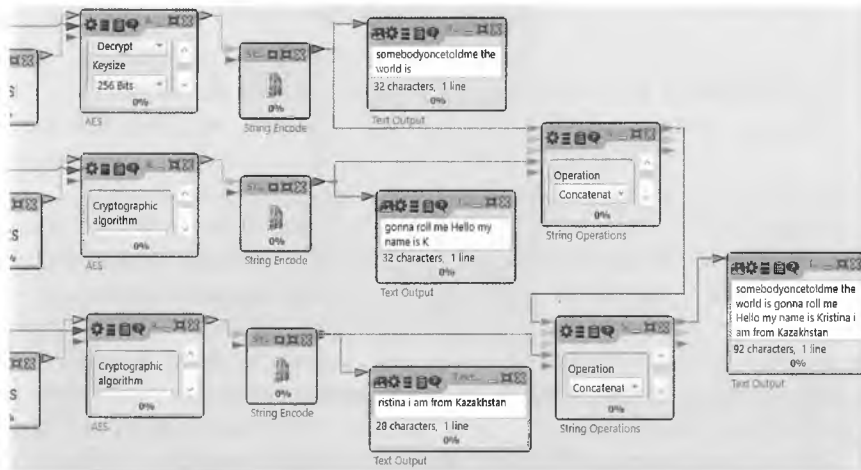


Рисунок 3.19 – Часть схемы с дешифрованием

Пояснение схемы:

1) Подаем на входы блоков дешифрации зашифрованное сообщение и ключи (разумеется, те же, что и были при шифровании).

2) Получаем 3 дешифрованные части сообщения и объединяем эти строки в одну строку с помощью операции Concatenation блока String Operations. В итоге получаем наше исходное сообщение.

3.3.2 Реализация режима шифрования CBC на AES.

В режиме CBC (Cipher Block Chaining – сцепление блоков шифротекста) на вход необходимо подать само шифруемое сообщение, ключ шифрования (для AES-128 - 128-битный) и вектор инициализации (для AES-128 - также 128-битный). На рисунке 3.20 представлены настройки режима. Обратите внимание, что для «ручной реализации» CBC использован режим ECB.



Рисунок 3.20 – Выбор параметров AES

Схема режима CBC представлена на рисунке 3.21.

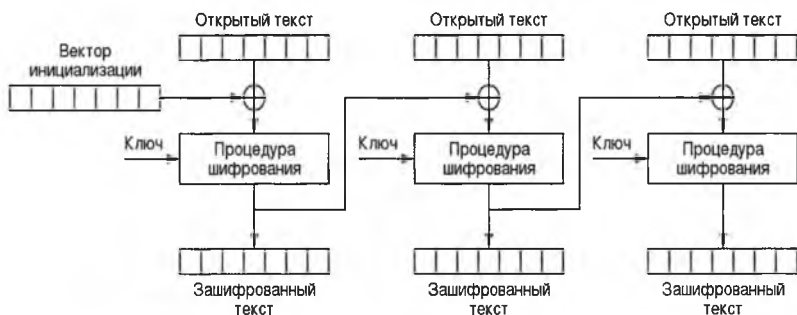


Рисунок 3.21 – Схема шифрования в режиме CBC

Видно, что шифруемый текст и вектор инициализации подвергаются операции XOR, а затем вместе с ключом поступают на вход для шифрации. Далее полученный блок и следующий шифруемый блок также подвергаются операции XOR и т.д. до тех пор, пока не будут задействованы все блоки.

Реализуем схему режима CBC на примере AES-128 по следующим шагам:

- 1) Разделим вручную исходное сообщение на 16-байтные блоки;
- 2) Возьмем первый блок и сгенерированный случайным образом вектор инициализации, обрабатываем их операцией XOR

и подаем на вход блока шифрования в качестве входного сообщения;

3) Подаем 128-битный ключ;

4) Выберем второй блок открытого текста и XOR-им его с полученным на предыдущем шаге зашифрованным блоком, шифруем его и т.д.

Для реализации части с первым блоком в среде Cryptool2 на вход сообщения подается результат операции XOR между шифруемым текстом и вектором инициализации. На вход ключа – подается 16-байтный ключ, а на вход сообщения – 16-байтная подстрока из исходной строки.

Для начала разделим исходное сообщение по 16 байтов, почти так же, как выполнялось в предыдущем пункте при реализации режима ECB (см. рисунок 3.22). Исходное сообщение выберем размером 32 байта. Пояснения к схеме аналогичны пояснениям к схеме на рисунке 3.22.

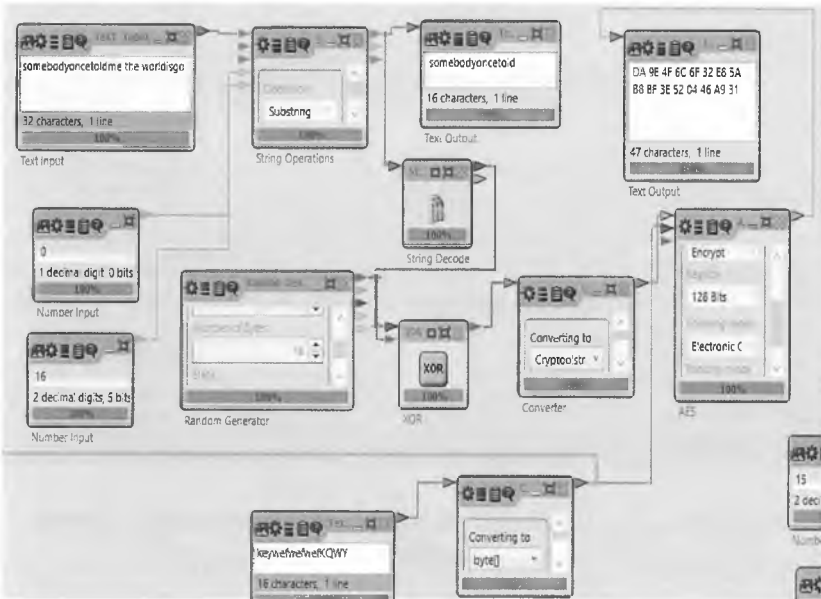


Рисунок 3.22 – Часть схемы с шифрованием первого блока сообщения

Пояснения к рисунку 3.22:

1) Отделяем от исходного сообщения первые 16 символов (2 блока Number Input и блок String Operations с операцией Substring());

2) Полученную подстроку XOR-им со случайной 16-байтовой числовой последовательностью (то есть с вектором инициализации) и полученный результат подаем на вход блока шифрования в качестве входного сообщения;

3) Подаем на вход блока шифрования ключ.

Так как в данном режиме шифруемые блоки связаны между собой, схема шифрации второго блока будет выглядеть так, как показано на рисунке 3.23.

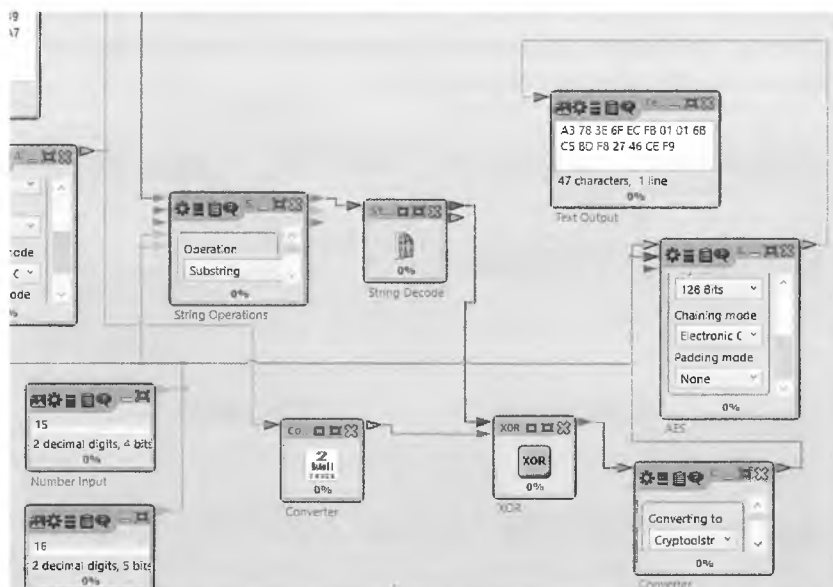


Рисунок 3.23 – Часть схемы с шифрованием второго блока сообщения

Пояснения к рисунку 3.23:

1) Подаем на вход второго блока шифрования тот же ключ, что и на первый;

2) После шифрации, продемонстрированной на рисунке 12, получился блок шифрованного текста. Пропускаем его через

конвертер для получения байтового массива и полученный массив байтов зашифрованного блока XOR-им с байтовым массивом, полученным из открытого текста текущего блока сообщения;

3) Полученный в результате XOR-а результат подаем на вход блока шифрования как входное сообщение.

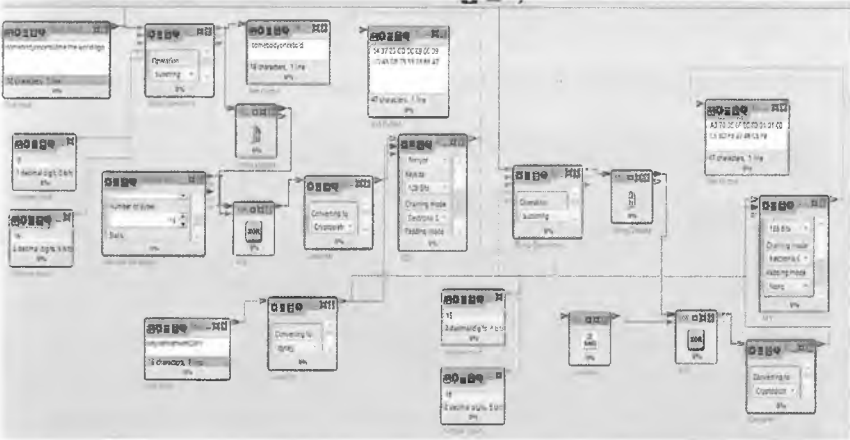


Рисунок 3.24 – Полная схема шифрования

Далее продемонстрируем дешифрование в режиме ECB. В целях упрощения схемы в данном и о всех последующих режимах шифруем и дешифруем только один 16-байтный блок сообщения. Схема дешифрования представлена на рисунке 3.25.

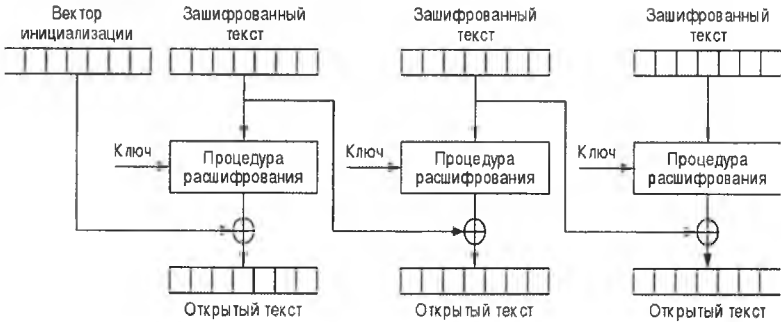


Рисунок 3.25 – Схема дешифрования в режиме CBC

Пояснения к схеме на рисунке 3.26:

- 1) Пояснения к части схемы с шифрованием блока сообщения аналогичны пояснениям к схеме на рисунке 3.22;
- 2) На вход ключа в блок дешифрации подаем наш ключ, а на вход сообщения – зашифрованное сообщение;
- 3) Полученный после дешифрации результат пропускаем через Конвертер для превращения в байтовый массив и XOR-им его с вектором инициализации;
- 4) Полученный байтовый массив переводим в строку и получаем исходное сообщение.

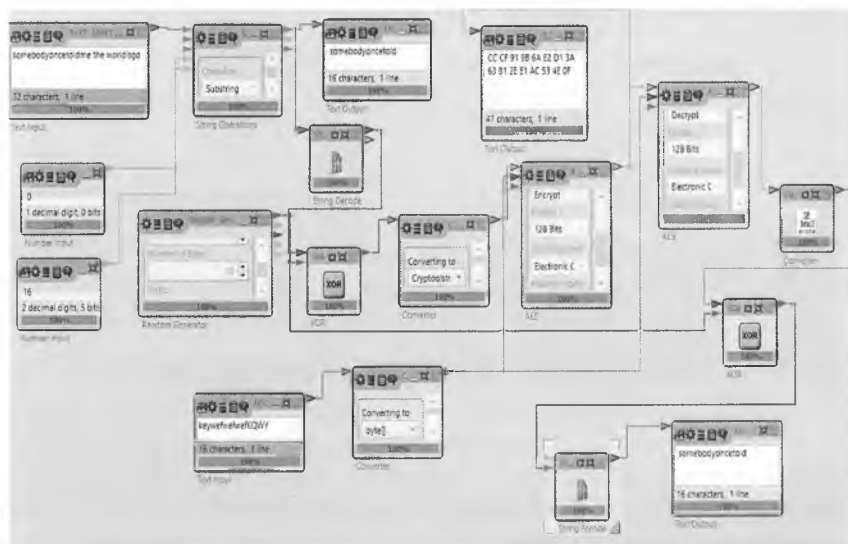


Рисунок 3.26 – Полная схема шифрование и дешифрования

Для проверки того, насколько правильно реализована схема, протестируем схему, продемонстрированную на рисунке 3.26 (схема шифрования и дешифрования). Для этого в том же файле, что и данная схема, реализуем тот же режим CBC, но уже готовый, который получается только подключением входных данных и настройкой самого блока AES.

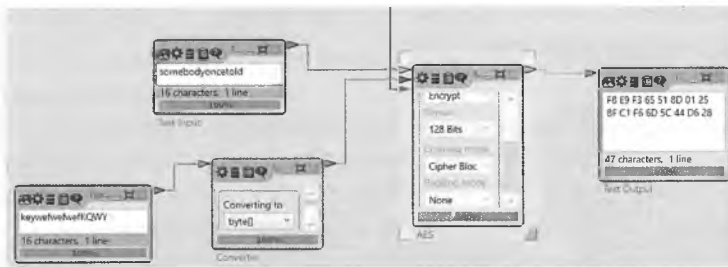


Рисунок 3.27 – Проверка правильности шифрации
 Пояснения к схеме на рисунке 3.27:

- 1) Добавляем готовый блок AES в режиме CBC и подаем на входы те же данные, что и для схемы выше;
- 2) Проверяем выведенный результат шифрования на соответствие с результатом нашей схемы.
- 3) Результаты шифрования одинаковы (рисунок 3.28) значит, шифрование и дешифрование выполнено верно.

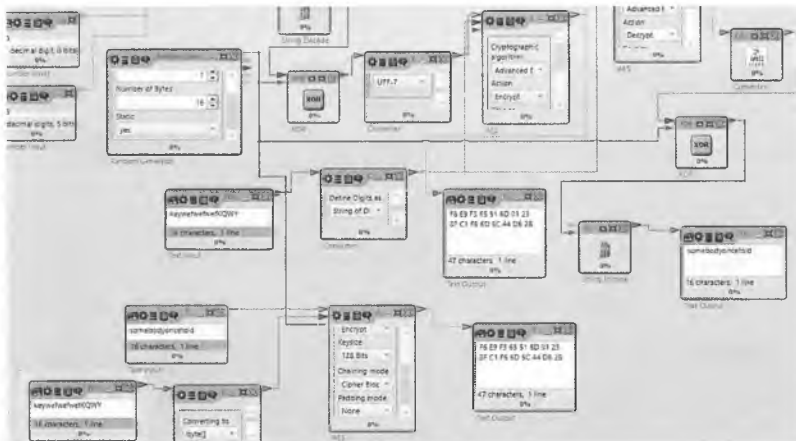


Рисунок 3.28 – Проверка правильности шифрования

3.3.3 Реализация режима шифрования CFB на AES.

Режим CFB (Cipher Feedback) – это режим обратной связи по шифротексту или режим гаммирования с обратной связью, в котором во время шифрования каждый блок открытого текста складывается по модулю 2 с блоком, зашифрованным на

предыдущем шаге. Схема шифрования в режиме CFB представлена на рисунке 3.29.

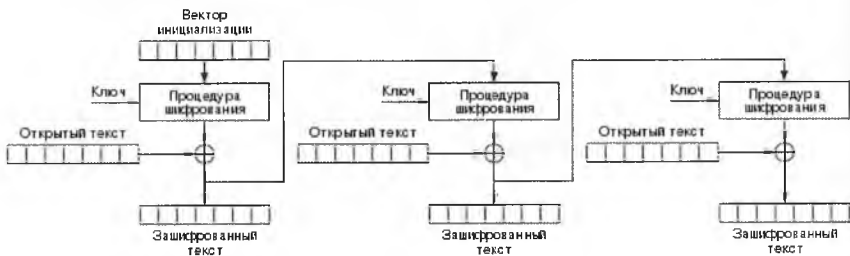


Рисунок 3.29 – Схема шифрования в режиме CFB

Для демонстрации шифрования в качестве входного сообщения будет выступать 32-байтная строка, разделенная по 16 байтов (соответственно, шифрование будет проходить в 2 этапа). Далее этот пункт при пояснениях схем будет опускаться. Схема с шифрованием первого 16-байтного блока строки представлена на рисунке 3.30.

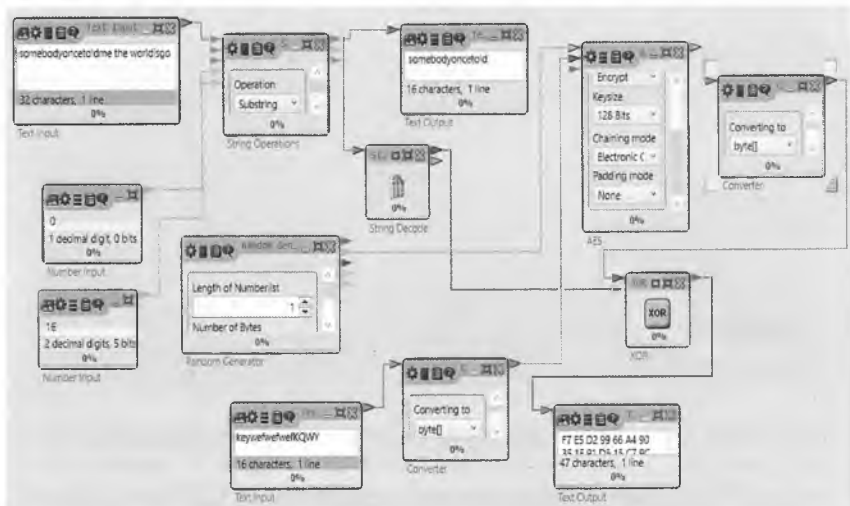


Рисунок 3.30 – Часть схемы с шифрованием первого блока сообщения

Пояснения к схеме на рисунке 3.30:

1) На вход блока шифрации подаем 16-байтный вектор инициализации и ключ;

2) Результат шифрования (последовательность, полученную на выходе блока шифрации), преобразуем в байтовый массив и XOR-им с блоком открытого текста;

3) В результате получаем последовательность, которая и будет являться шифрованным сообщением.

Добавляем к данной схеме второй этап шифрования (то есть шифрование второго блока сообщения).

Пояснения к схеме на рисунке 3.31:

1) На вход блока шифрации подаем шифрованный текст, полученный в результате шифрования первой части сообщения (см. рисунок 20) и ключ;

2) Результат шифрования, преобразуем в байтовый массив и XOR-им с блоком открытого текста;

3) В результате получаем последовательность, которая и будет являться шифрованным сообщением.

Общая схема шифрования представлена на рисунке 3.32.

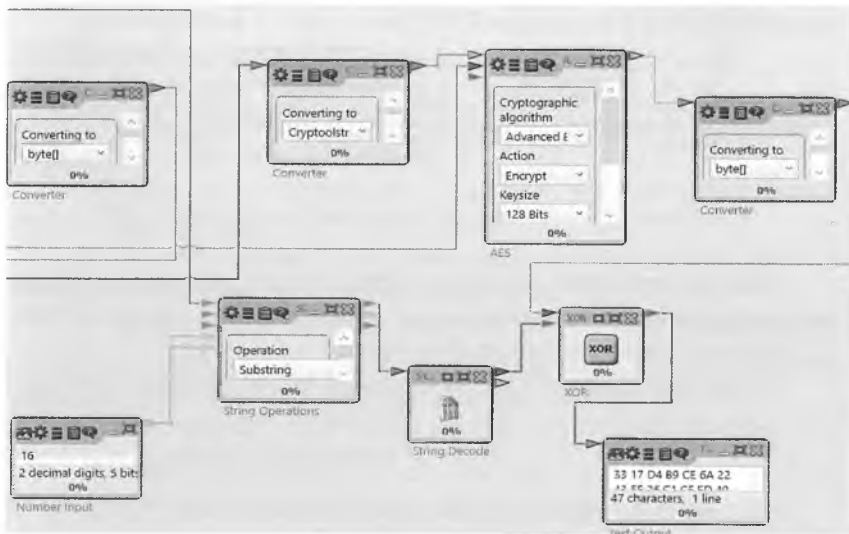


Рисунок 3.31 – Часть схемы с шифрованием второго блока сообщения

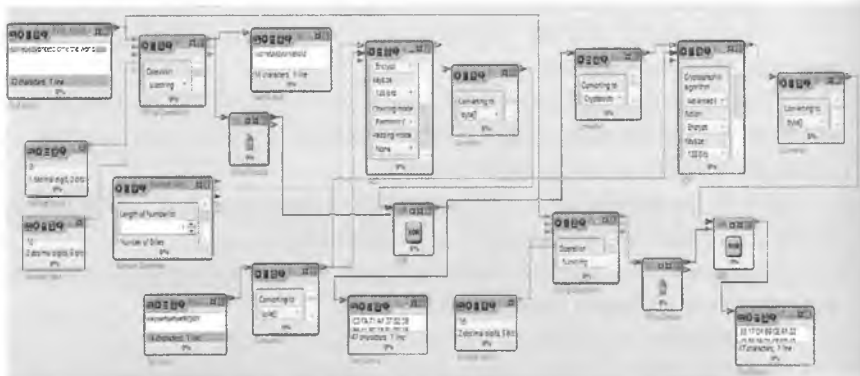


Рисунок 3.32 – Полная схема шифрования

Схема дешифрования в режиме CFB представлена на рисунке 3.33.

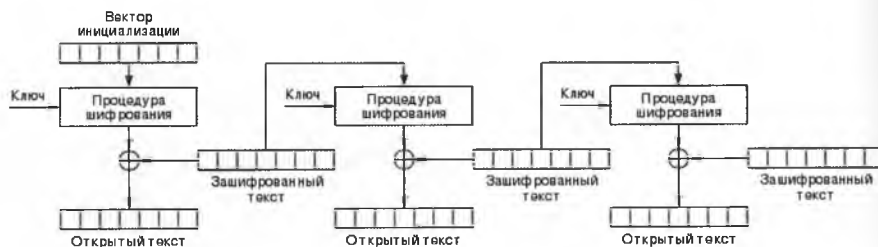


Рисунок 3.33 – Схема дешифрования в режиме CFB

Как и в примере с режимом CBC, в целях упрощения схемы продемонстрируем шифрование и дешифрование только одного 128-битного блока сообщения (алгоритмом AES-128).

Реализация данной схемы представлена на рисунке 3.34.

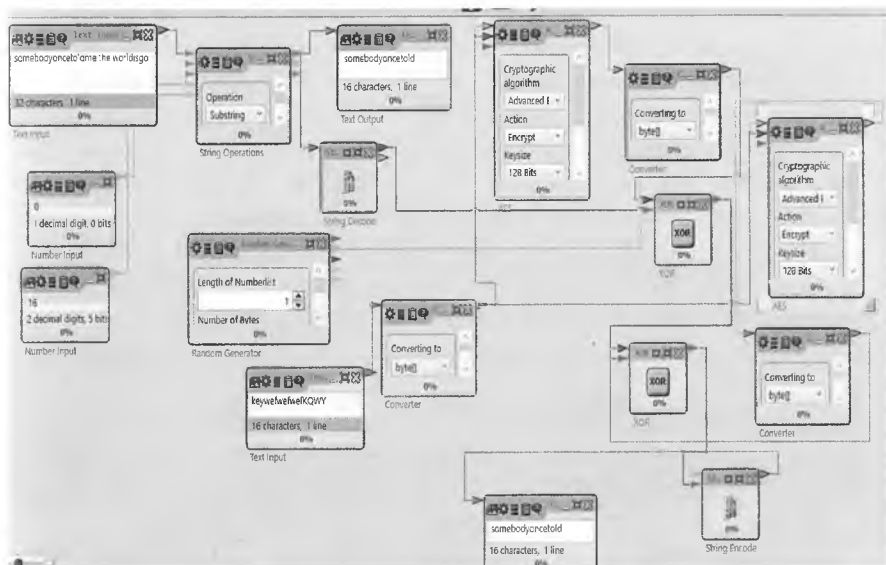


Рисунок 3.34 – Полная схема шифрования и дешифрования

Пояснения к схеме на рисунке 3.34:

- 1) Пояснения к части схемы с шифрацией блока сообщения аналогичны пояснениям к схеме на рисунке 3.30;
- 2) В данной схеме результат «верхнего» XOR-а – это зашифрованное 16-байтное сообщение, а результат «нижнего» XOR-а – дешифрованное сообщение;
- 3) Даже для дешифрования в данном режиме используется не блок дешифрации, а блок шифрации;
- 4) На вход ключа в блок дешифрации подаем наш ключ, а на вход сообщения – вектор инициализации;
- 5) Полученный после шифрации (а не дешифрации) результат пропускаем через Конвертер для превращения в байтовый массив и XOR-им его с зашифрованным текстом;
- 6) Полученный байтовый массив переводим в строку и получаем исходное сообщение.

3.3.4 Реализация режима шифрования OFB на AES.

Режим OFB (Output Feedback) – это режим обратной связи, когда блок вывода превращает блочный шифр в синхронный

шифр потока: он генерирует ключевые блоки, которые являются результатом сложения с блоками открытого текста, чтобы получить зашифрованный текст. Так же, как с другими шифрами потока, зеркальное отражение в зашифрованном тексте производит зеркально отражённый бит в открытом тексте в том же самом местоположении. Это свойство позволяет многим кодам с исправлением ошибок функционировать как обычно, даже когда исправление ошибок применено перед кодированием.

Схемы шифрования и дешифрования в режиме OFB представлены на рисунках 3.35 и 3.36 соответственно.

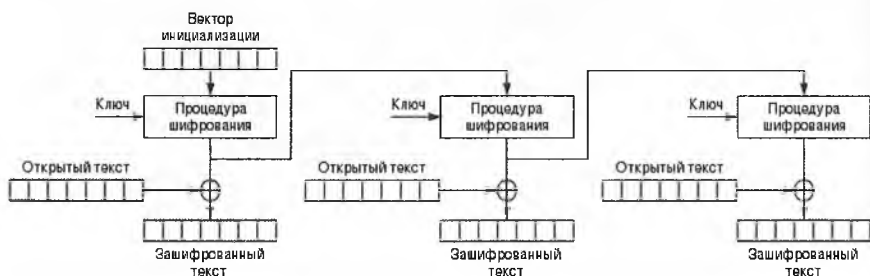


Рисунок 3.35 – Схема шифрования в режиме OFB

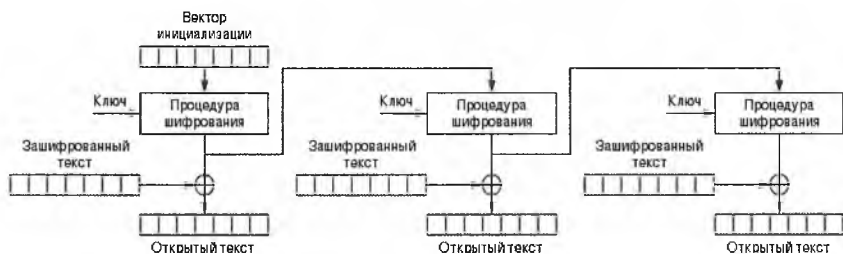


Рисунок 26 – Схема дешифрования в режиме OFB

Шифрование в режиме OFB абсолютно идентично шифрованию в режиме CFB (рисунок 3.29). А это значит, что и реализации данной схемы в Cryptool2 будут одинаковыми.

Шифрование в режиме OFB представлено на рисунках 3.37-3.39.

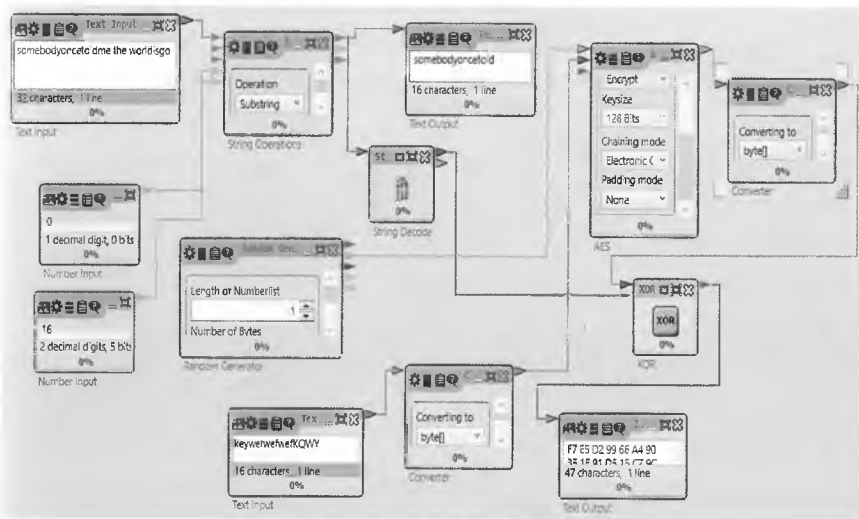


Рисунок 3.37 – Часть схемы с шифрацией первого блока сообщения

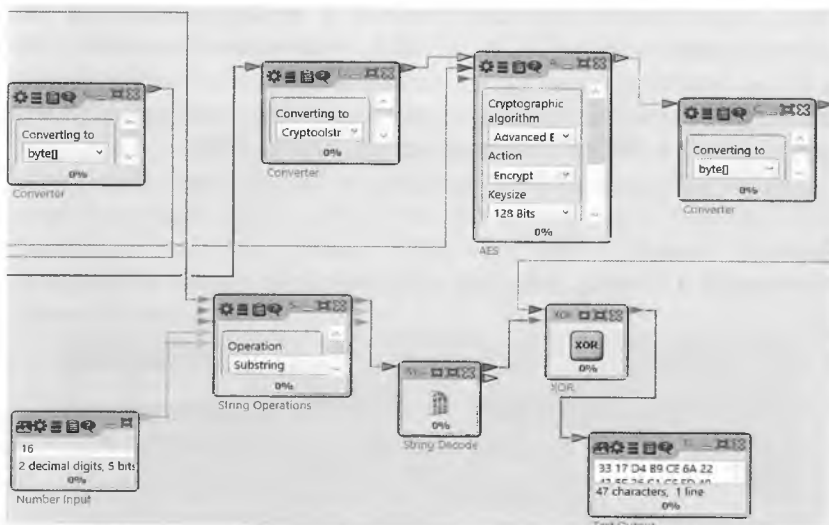


Рисунок 3.38 – Часть схемы с шифрацией второго блока сообщения

Пояснение к схеме на рисунках 3.38 и 3.39 аналогичны пояснениям к схемам на рисунках 3.30 и 3.31 соответственно.

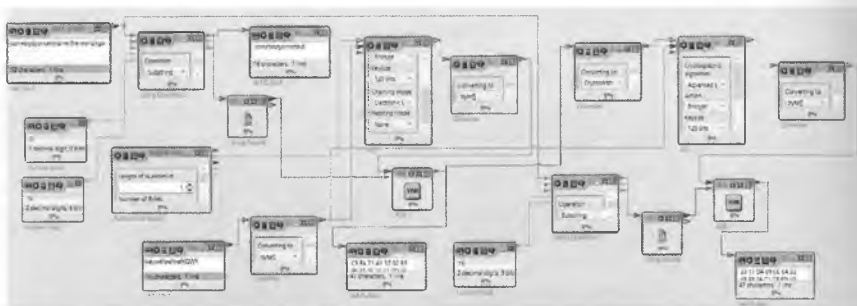


Рисунок 3.39 – Полная схема шифрования

Обратимся к рисунку 3.36 и рассмотрим схему дешифрования в режиме OFB. Очевидно, что первый шаг дешифрации совпадает с первым шагом дешифрации в режиме CFB. А для реализации шифрования и дешифрования как раз берется только один 16-байтный блок сообщения. Это значит, что в схеме дешифрования будет задействован только первый этап схемы на рисунке 3.37. Иначе говоря, данный пример дешифрации в OFB аналогичен дешифрации в CFB.

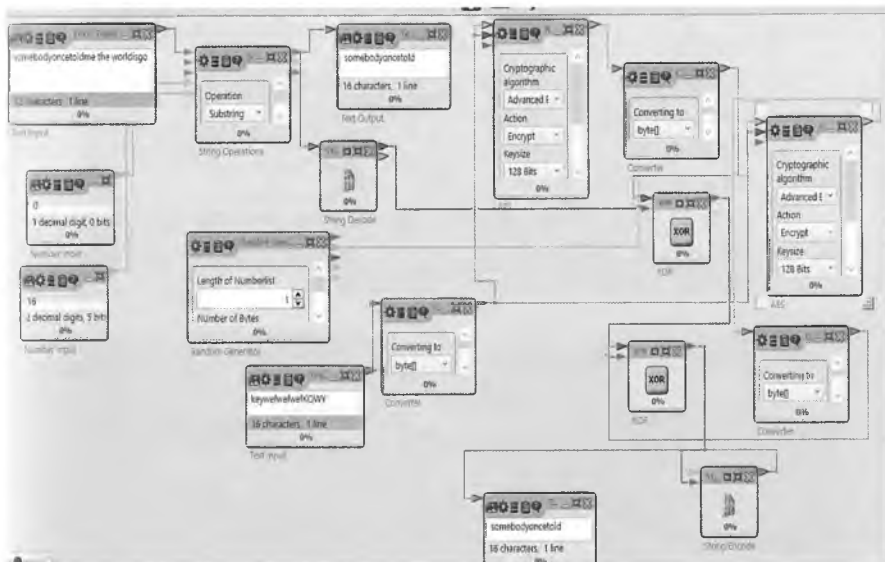


Рисунок 3.40 – Полная схема шифрования и дешифрования

Пояснения к рисунку 3,40 будут аналогичны пояснениям к рисунку 3.34.

Как и в случае с проверкой режима CBC, для проверки того, насколько правильно реализована схема, протестируем схему, продемонстрированную на рисунке 3.40 (схема шифрования и дешифрования). Для этого в том же файле, что и данная схема, реализуем тот же режим OFB, но уже готовый, который получается только подключением входных данных и настройкой самого блока AES.

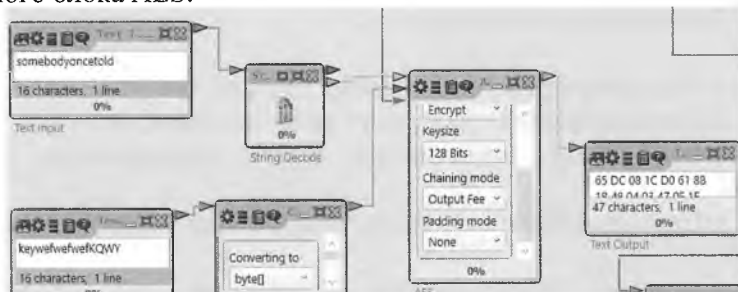


Рисунок 3.41 – Проверка правильности шифрации

Пояснения к схеме на рисунке 3.41:

- 1) Добавляем готовый блок AES в режиме OFB и подаем на входы те же данные, что и для схемы выше;
- 2) Проверяем выведенный результат шифрования на соответствие с результатом нашей схемы.
- 3) Результаты шифрования одинаковы, значит, шифрование мы выполнили верно. А если верно шифрование, то дешифрование также выполнено правильно.

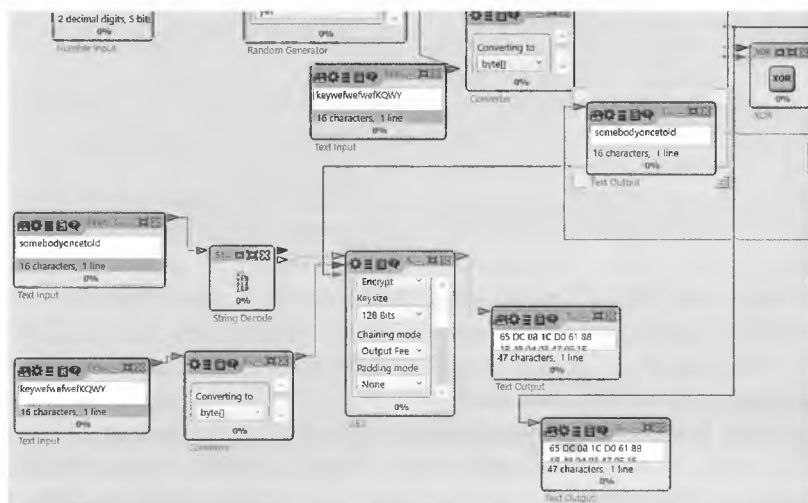


Рисунок 3.42 – Проверка правильности шифрования

Вопросы для самоконтроля:

- 1 Что собой представляет шифр Цезаря?
- 2 Принцип работы частотного криптоанализа?
- 3 Что собой представляет режим шифрования ECB алгоритма AES?
- 4 Принцип работы режима шифрования CBC алгоритма AES?
- 5 Принцип работы режима шифрования OFB алгоритма AES?

6 Принцип работы режима шифрования CFB алгоритма AES?

7 Как произвести шифрование по алгоритму RSA?

8 Принцип дешифрования по алгоритму RSA?

9 Принципы криптоанализа алгоритма RSA?

10 Как произвести проверку шифрования режима шифрования OFB алгоритма AES в среде Cryptool2?

11 Как произвести проверку шифрования алгоритма RSA в среде Cryptool2?

4 ПРАКТИЧЕСКИЕ АСПЕКТЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПРИМЕНЕНИЕМ ПРОГРАММ OPNET MODELER И WIRESHARK

4.1 Установка и изучение программной среды Opnet Modeler v.14 на примере проектирования локальной беспроводной сети и атаки на разработанную сеть с помощью Wireshark

Программные системы моделирования сетей является инструментом, который можно использовать проектировщикам сети при проектировании новой сети или вынесении существенных модификаций в уже функционирующую. Результаты предоставленной категории разрешают испытать итоги введения тех или иных решений еще до уплаты покупаемого оборудования. Большинство программных пакетов стоят довольно дорого, но и итоговая экономия может быть весьма существенной. Поэтому проблема рассмотрения, анализа и выбора пакета программ для построения сетей считается актуальной [12].

В настоящее время имеется целая последовательность известных систем имитационного моделирования разнообразного класса - от элементарных программ, назначенных для введения на индивидуальном компьютере, до больших систем, имеющие библиотеки многих имеющихся на продаже устройств по отрасли связи и допускающих в большой степени провести автоматизацию исследований анализируемой сети.

OPNET IT Guru рекомендуют для организации виртуальной сети, моделирующей состояние подлинных сетей, применяющих маршрутизаторы, коммутаторы, протоколы, серверы, и собственные приложения.

Семейство OPNET - рекомендуют для построения и моделирования различных сетей, в том числе компьютерных систем, приложений и разделенных систем. Дает возможности ввода и наоборот вывода информации - данных о структуре и сетевой нагрузке [13].

Учитывая перечень выполняемых функций и обширную библиотеку по виртуальным сетевым оборудованьям, и

обеспечение проверки на безопасность структуры построения сети для имитационного моделирования из семейства пакета программ OPNET IT Guru выбираем OPNET Modeler 14 версии.

Opnet Modeler - это удобное программное обеспечение, которое может быть использовано для решения многих задач, например, для проверки протоколов связи, анализа взаимодействий протоколов, оптимизации и планирования сети. Также возможно осуществить с помощью программы проверку правильности аналитических моделей и описание протоколов.

После окончания моделирования пользователь получает в свое распоряжение следующие характеристики по производительности сети:

- прогнозируемые задержки между конечными и промежуточными узлами сети, пропускные способности каналов, коэффициенты использования сегментов, буферов и процессоров;
- пики и спады трафика как функцию времени, а не как усредненные значения;
- источники задержек и узких мест сети.

Wireshark - программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других. Он разработан для отображения информации между уровнями 2-7 модели OSI. С помощью Wireshark можно осуществлять наблюдение за сетевым трафиком например организации в режиме действительного времени, позволяющим выявлять проблемы, вести анализ и реализовать еще дополнительные задач, обеспечивающих необходимую работу сетевой среды. Wireshark имеет графический пользовательский интерфейс. Функциональность, которую предоставляет Wireshark, очень схожа с возможностями программы tcpdump, однако Wireshark имеет графический пользовательский интерфейс и гораздо больше возможностей по сортировке и фильтрации информации. Программа позволяет пользователю просматривать весь проходящий по сети трафик в режиме реального времени, переводя сетевую карту в неразборчивый режим.

Стоит отметить, что утечка личных данных или перехват трафика может серьезно сказать, что может серьезно сказаться не только репутации одного человека и огромных корпораций, но и на возможности дальнейшего существования личностей. А в результате построения моделей на определенном программном

обеспечении позволяет найти определенные уязвимости сети и устранить их либо снизить риски утечки важной информации.

Можно выделить следующие особенности Wireshark:

- 1) Доступность для систем Windows и Unix.
- 2) Возможность фильтрования пакетов с принятыми критериями.
- 3) Возможности захватить пакетные снимки в сетевом интерфейсе.
- 4) Возможности импортировать пакеты в текстовом формате.
- 5) Возможность поиска пакетов, устанавливая ряд критериев.

Для запуска Wireshark в среде Windows требуется следующее:

- 400 МБ ОЗУ;
- запуск на любой Windows версии, как на уровне сервера, так и на рабочем столе;
- 300 МБ на жестком диске.

Перед началом работы с любым программным обеспечением необходимо, это программное обеспечение установить. Ornet является платно-распространяемой программой, поэтому способ установки отличается от установки Wireshark, которая распространяется бесплатно и имеет один установочный файл.

Устанавливать Ornet лучше всего в Виртуальную машину на основе 32 разрядной системы, однако можно установить и в 64 разрядной системы Windows. Установка в ВМ позволяет избежать ошибки блокировки нежелательного программного обеспечения и его блокировка установки, также это можно избежать через редактор реестра. После окончательной установки необходимо настроить работу в качестве обучения, для этого переходим в настройки репозитории, находим сетевое моделирование, редактируем данную запись, перезаписав ее как stdmod (Рисунок 4.1).

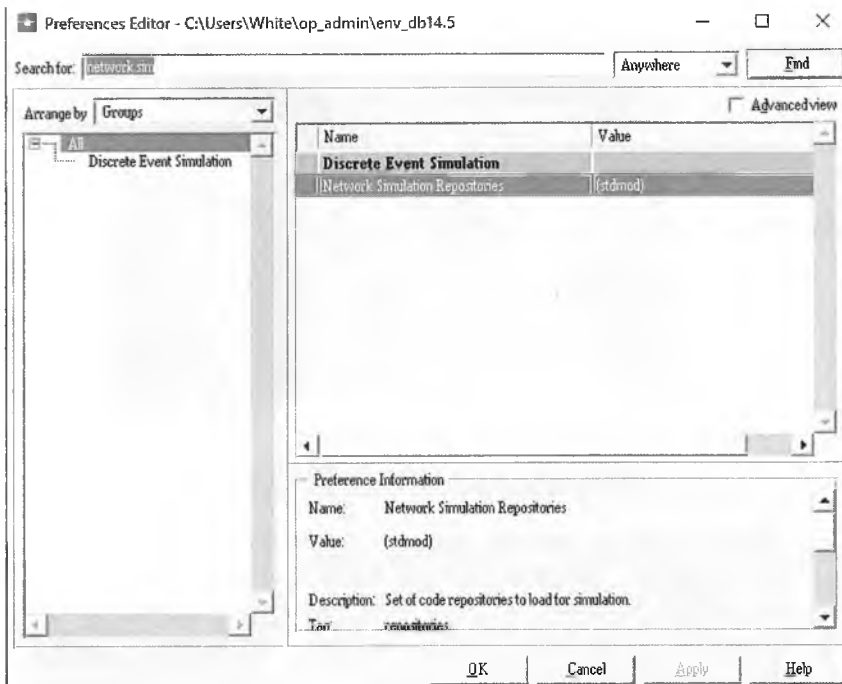


Рисунок 4.1 – Дополнительная настройка Ornet для начала работы

Теперь возможно начать работать с данной утилитой. Для этого необходимо зайти в создание нового проекта во вкладке создания и работы с Файлами. Здесь возможно изменить тип создаваемого файла, но так как создается проект беспроводной сети, изменения в данной вкладке вносить не нужно (Рисунок 4.2).

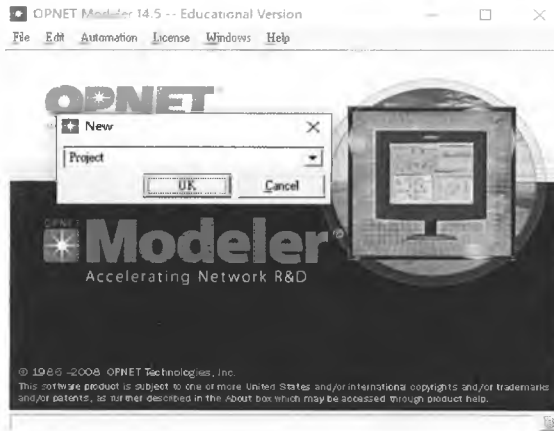


Рисунок 4.2 – Создание нового проекта

Перед началом работы проекту необходимо присвоить имя и имя сценария. Названия могут быть любыми к примеру, в данной работе названа WLAN1 (так как будет разворачиваться беспроводная локальная сеть), первого сценария в данной утилите, следовательно, название scenario 1 (Рисунок 4.3).

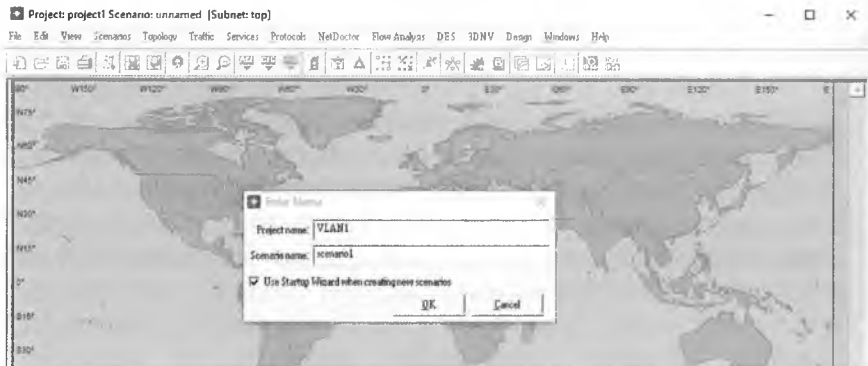


Рисунок 4.3 – присвоение названия проекту и сценарию

Далее выбирается размер сети, можно настроить размер сети от небольшой логической локальной сети, до мировой – глобальной сети. В данной работе нет необходимости в

гигантских или очень маленьких сетях поэтому выбранный тип будет Campus (Рисунок 4.4).

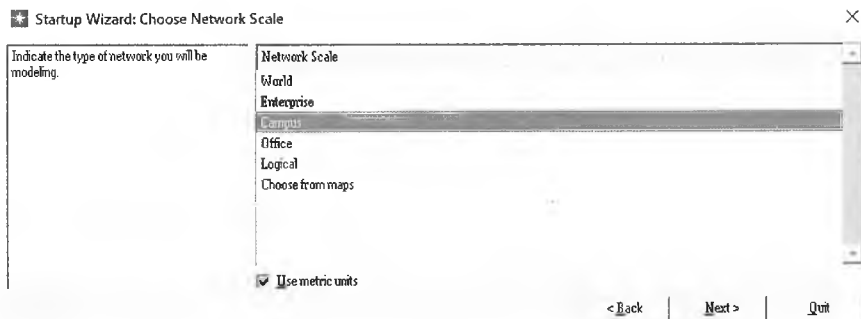


Рисунок 4.4 – Выбор размера сети

На следующем этапе выбираются конкретные размеры местности, на которой будет размещена проектируемая сеть. В зависимости от планируемого размера и корректируется область. Возможно подобрать размер от нескольких метров и футов, до нескольких километров и градусов. Создается квадратный кампус размерами 500 на 500 метров (Рисунок 4.5).

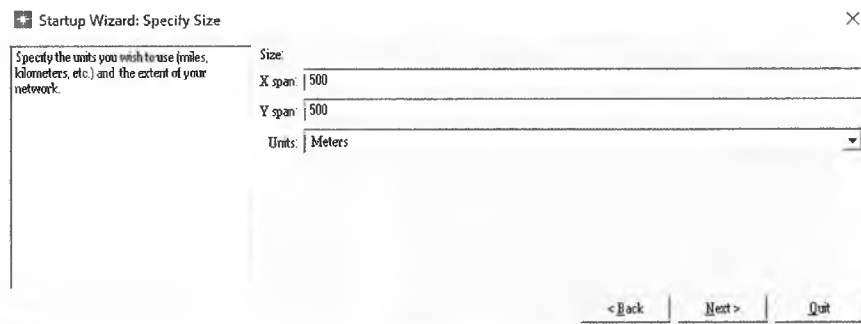


Рисунок 4.5 – Размеры сети

Далее рекомендуется выбрать типы оборудования и элементов сети, которые будут размещены в области проектирования сети. Это можно не делать так как палитра

предоставляет постоянный доступ ко всем устройствам, прописанных в утилите. Но для удобства выбирается необходимый пакет устройств и он автоматически добавляется в первую папку устройств по умолчанию (Рисунок 4.6).

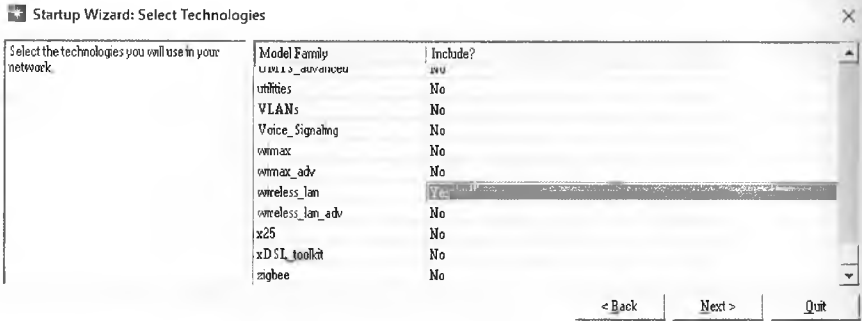


Рисунок 4.6 – Пакет необходимых устройств в панели быстрого доступа

После предварительной настройки и подтверждения окончания предварительной настройки, открывается рабочая область, куда будут размещаться устройства, а поверх этой области автоматически открыта палитра доступных устройств (Рисунок 4.7).

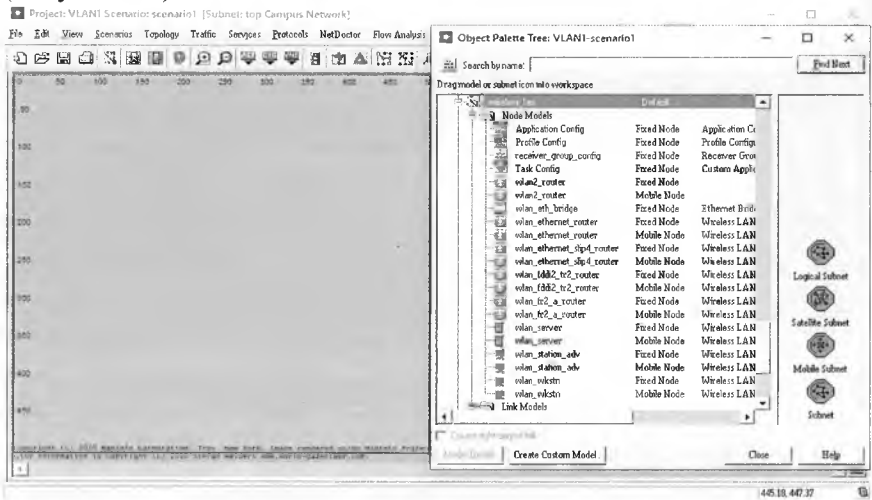


Рисунок 4.7 – Палитра устройств OPNET

Набор элементов можно изменить путем перехода в палитру «Configure Palette». Для добавления элементов на рабочую область необходимо переносить их из палитры. Для этого выбирается элемент в палитре щелчком левой кнопки мыши, вторым аналогичным щелчком, но уже в рабочей области, добавляется элемент в рабочую область, также можно перетаскивать элементы из палитры. Дополнительно программой предусмотрена возможность создания комбинированных элементов из шаблонов.

Модель сети создается с помощью редактора с использованием узлов (nodes) и каналов связи (links) из базы ресурсов (окно с изображениями узлов и связей, Object Palette). Ниже в таблице 4.1 представлены элементы использованные в работе, основная папка где их можно найти в палитре.

Таблица 4.1 – Элементы проектируемой сети

Кол-во	Компонент	База ресерсов	Описание
24	wlan_wkstn (Fixed node)	wireless_lan	Компьютеры (фиксируемый узел)
4	wlan_wkstn (Mobile node)	wireless_lan	Компьютеры (мобильный узел)
1	ethernet server	internet toolbox	Сервер
2	ethernet16 switch	internet toolbox	Коммутатор
1	ethernet4 slip_gtwy	internet toolbox	Маршрутизатор
2	wlan_ethernet_router	wireless_lan	Wireless LAN и Ethernet IP Router
5	100BaseT	internet toolbox	Соединительные линии
1	Application Config	wireless_lan	Определяет стандартные и пользовательские приложения, используемые в имитационном моделировании, включая параметры трафика и качества обслуживания
1	Profile Config	wireless_lan	Определяет режимы использования приложений пользователями группой пользователей

На рисунке 4.8 представлена схема, на которой размещены все необходимые элементы, это 28 персональных компьютеров

(24 статических и 4 подвижных, которые будут менять положение с определенной скоростью и по определенной скорости), 1 сервер, маршрутизатор, роутер раздачи беспроводной сети, 2 коммутатора, один определитель профилей и один определитель активности пользовательских приложений.

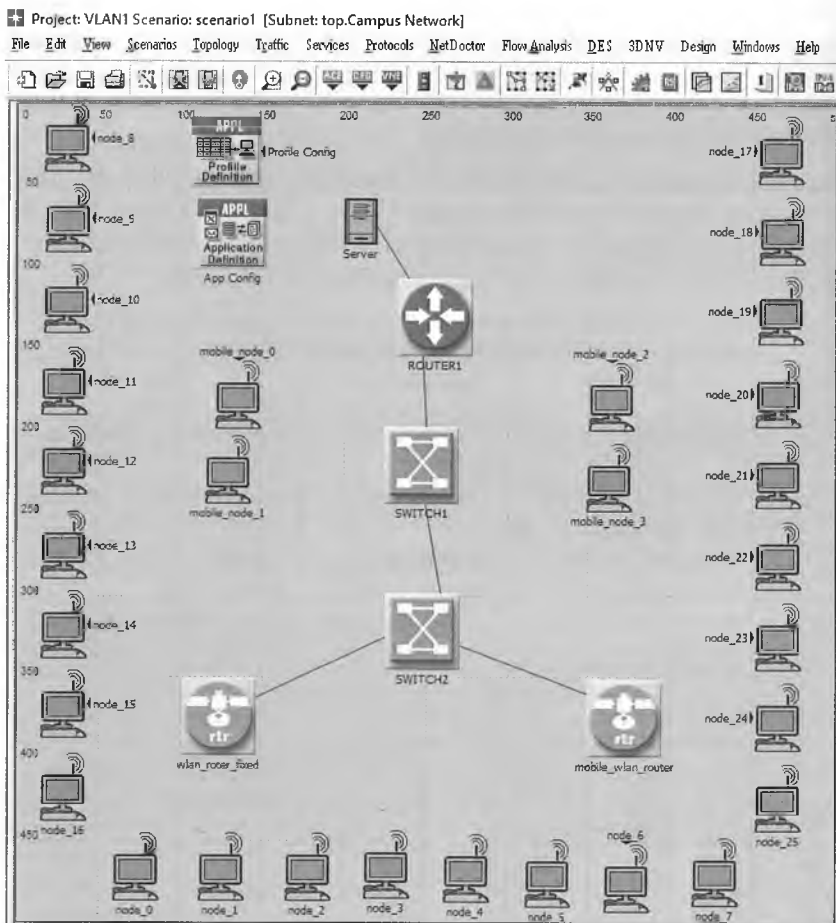


Рисунок 4.8 – Архитектура проектируемой сети

4.1.1 Настройка пользовательских приложений и их профилей.

Для настройки оборудования необходимо нажать правой клавишей мыши на интересующем оборудовании и выбрать в меню пункт «Edit Attributes» в зависимости от выбора оборудования в рабочей области появится окно с различным набором настраиваемых параметров.

Настройка параметров приложения и профиля «Тип трафика» задается с помощью элемента палитры «Application Definition».

Элемент «Application Definition» необходимо перенести из палитры в рабочую область и разместить рядом с сервером. «Application Definition» содержит характеристики приложений, создаваемых в виде потоков и имеющих собственные параметры трафика.

Для создания потоков на «Application Definition» нужно перейти в меню «Edit Attributes», и для примера создадим 3 стандартных потоков для разных случаев. Сюда входит доступ к базам данных, обработка электронной почты, передача файлов, работа в Интернете. Также можно создать другие, но для данной работы в этом нет особой необходимости (Рисунок 4.9).

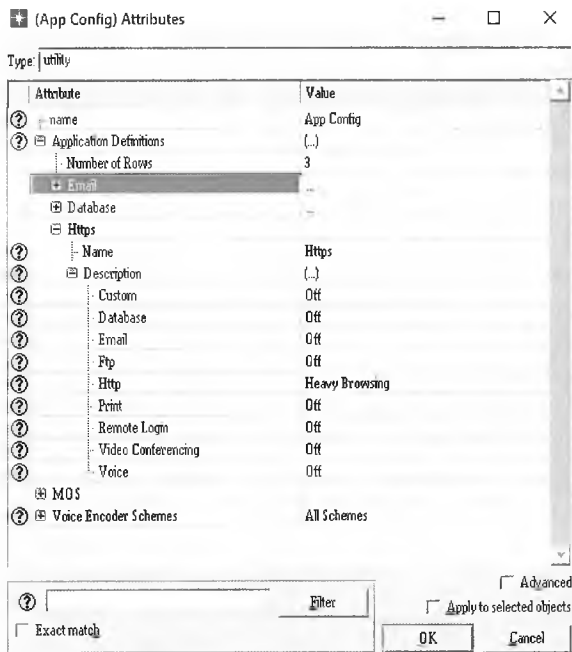


Рисунок 4.9 – Создание приложений пользовательской активности

После создания потоков приложений необходимо сконфигурировать профили пользователей, работающих в спроектированной сети. Эту функцию выполняет элемент палитры «Profile Definition».

Каждому профилю дается название и описывается ряд пользовательских характеристик: время начала работы, продолжительность, окончание, интенсивность его пребывания и работы в сети и какими из предложенных (созданных) приложений он пользуется.

Указанные параметры задаются аналогично «Application Definition» через пункт меню «Edit Attributes» (Рисунок 4.10).

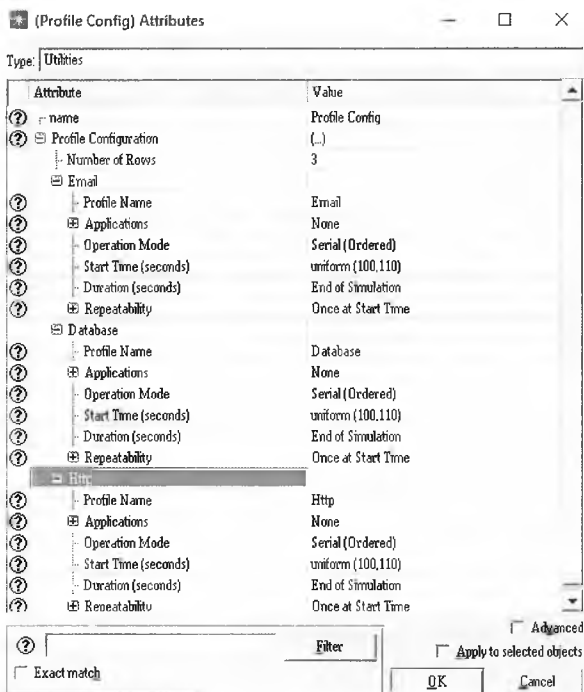


Рисунок 4.10 – Настройка профилей активности пользователей

4.1.2 Настройка сервера.

При настройке сервера нужно прописать тип трафика, генерируемого пользователями. Самые распространенные типы трафика: данные, речь, видео. Каждый из них предъявляет различные требования к передаче, обеспечению необходимого качества обслуживания, выделению достаточной пропускной способности. В зависимости от направления деятельности предприятия/фирмы по сети будет передаваться трафик различного рода. Соответственно при проектировании важно правильно рассчитать загрузку каналов и оборудования. Проверить расчеты позволяет моделирование планируемой нагрузки.

Тип собираемой статистики указывается также через пункт меню Choose Individual Statistics. Для сервера необходимо собрать определенные типы статистики (Рисунок 4.11):

- в пункте Animation под пунктом Анимация процессов (Process Anomation) пункты application, CPU, ip, mac;
- в пункте Node Statistic полностью пункт Application Demand (Traffic Sent, Traffic Received);
- полностью пункты Requesting Custom Application;
- полностью настройка сервера баз данных (Server DB);
- полностью настройка сервера электронных почт (Server Email);
- полностью настройка сервера протокол передачи файлов (Server Ftp);
- полностью настройка сервера http - протокол передачи данных (Server DB).

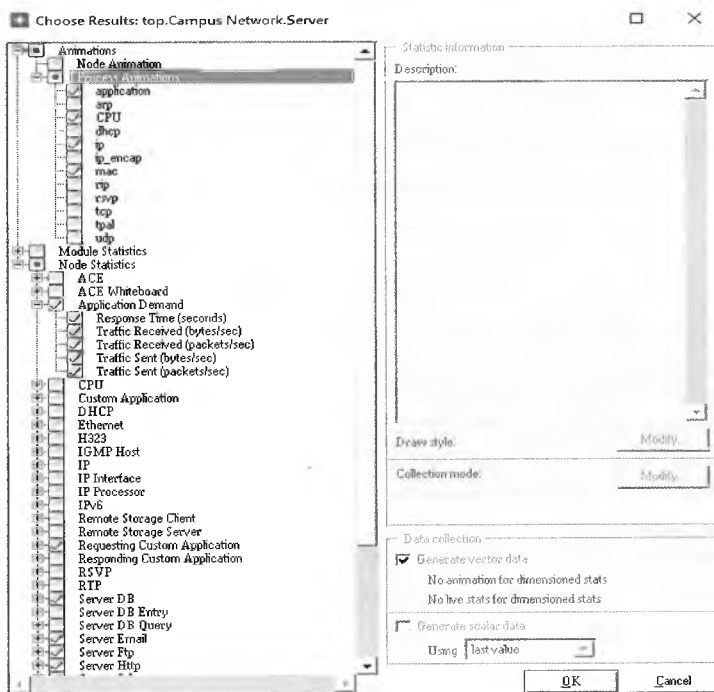


Рисунок 4.11 – Настройка Сервера

Также на Сервере необходимо подключить перейти в настройки меню Edit Attributes и включить активность приложений, используемых на рабочих станциях. Если приложений больше, то на сервере отмечается большее количество приложений, но у нас их три, поэтому отмечаем электронную почту, базы данных и интернет доступ (Рисунок 4.12).

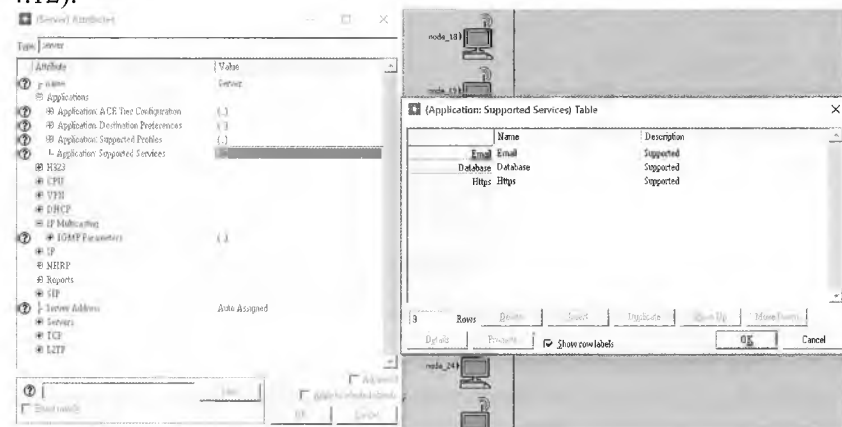


Рисунок 4.12 – Подключение приложений в интерфейсе сервера

4.1.3 Настройка Маршрутизаторов беспроводного подключения.

Для настройки параметров маршрутизатора необходимо перейти в настройки меню, выбрав графу «Edit Attributes». На диалоговом окне настроек параметров роутера задать имя беспроводной сети (BSS Identifier), осуществить выбор стандарта связи, скорость передачи (Data Rates) и другие свойства проектируемой сети (Рисунок 4.13). Для маршрутизатора обязательно собрать следующие статистические показатели: загрузка процессора, объем переданного, полученного, отброшенного трафика и т.д.

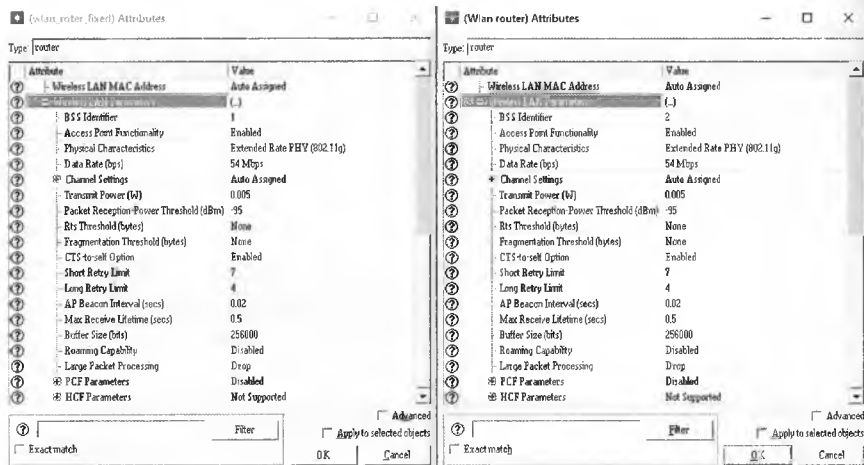


Рисунок 4.13 – Настройка Маршрутизаторов

4.1.4 Настройка Коммутаторов (Свитчей).

Как правило, дополнительная настройка коммутатора не требуется, если нет необходимости реконфигурации портов или настройки VLAN. Для коммутатора можно указать тип собираемой статистики – нажать правой кнопкой мыши на объект и выбрать графу «Choose Individual Statistic». Далее галочками выбрать интересующие параметры. Для коммутатора обязательно собрать следующие статистические показатели: объем трафика переданного, полученного, отброшенного.

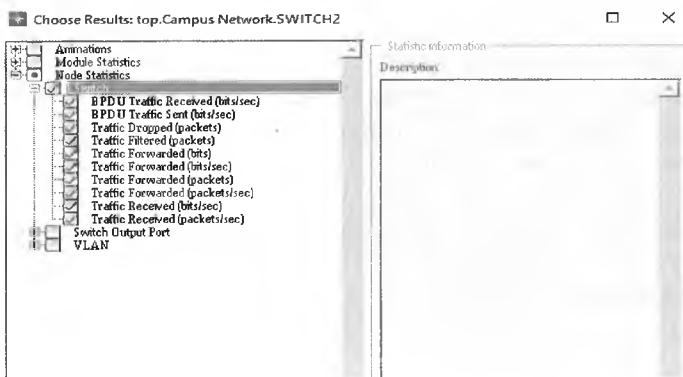


Рисунок 4.14 – Настройка Коммутатора

4.1.5 Настройка окончательных пользователей (рабочих станций – персональных компьютеров).

При настройке оборудования для конечных пользователей нужно указать название и тип пользователя. Конечный пользователь (рабочая станция) для WLAN сети может быть представлен двумя способами: фиксированный узел или мобильный узел.

Подключения конечных пользователей к маршрутизатору, происходит следующим образом. Выбираем пункт меню Edit Attributes: выбрать Wireless LAN - Wireless LAN Parameters на поле BSS Identifier укажет имя и параметры беспроводной сети и заполняется графа Application – Supported Profiles, указывающая, сколько и какого рода пользователей будут присутствовать в этой сети. Здесь аналогично серверу создаются потоки, учитывающие пользователей сети, на основе профилей, созданных в элементе рабочей области Profile Definition (Рисунок 4.15).

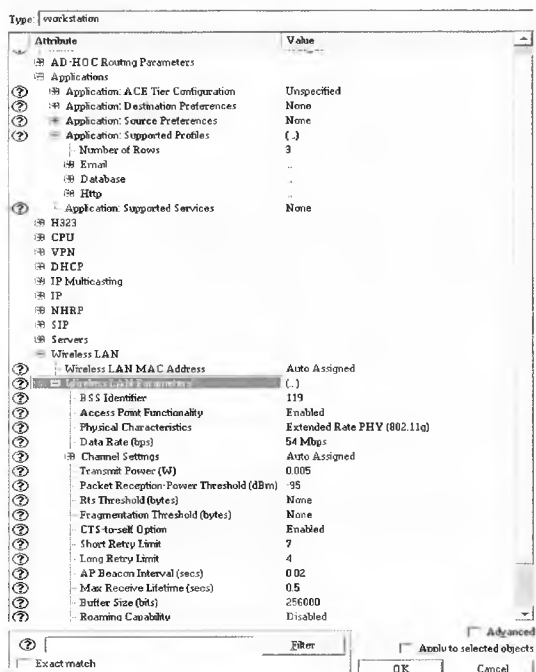


Рисунок 4.15 – Настройка ПК

4.1.6 Настройка движения мобильных станций.

Выбрать из меню пункт меню Topology выбираем создать траекторию движения мобильных станций (Define Trajectory) Прежде всего присваиваем траектории свое собственное имя, затем выбираем мобильную станцию, для которой решили выбрать траекторию на рабочей области и указать линий движений для мобильных рабочих станций и нажать Complete чтобы сохранить траекторию (Рисунок 4.16)

Также для каждой мобильной станции можно указать скорость движения по всей траектории, по определенному сегменту траектории. Для выбора траектории движения мобильной станции мы заходим в меню настройки Edit Attributes, где в пункте выбора траектории подключаем к определенному ПК определённое направление.

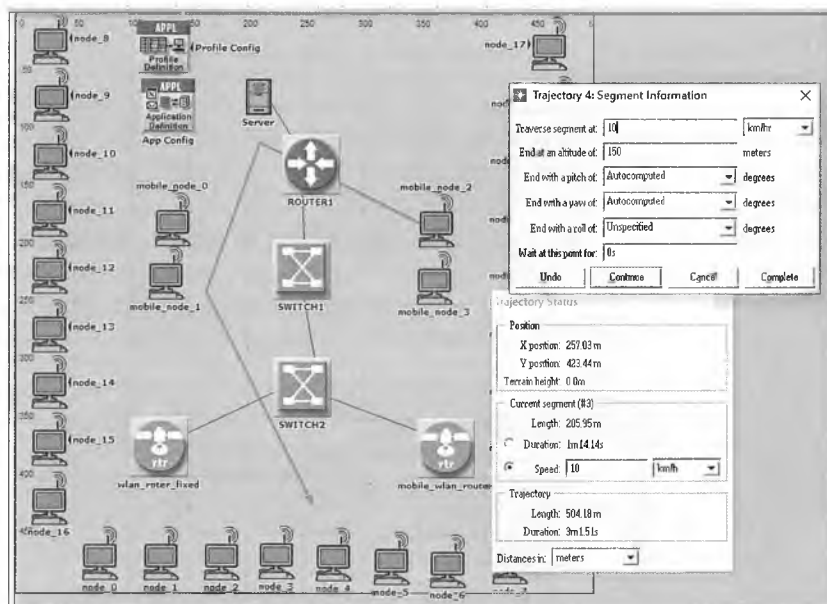


Рисунок 4.16 – Настройка траектории

Для конечных пользователей снять следующую статистику:

- задержку, вариацию задержки, объем трафика полученного, отправленного для типов приложений: Video Called Party, Video Calling Party, Voice Application;
- количество загруженных объектов/страниц (Downloaded Objects/Pages) для Client http;
- Размеры загруженных файлов (Downloaded File Size) и Downloaded Response Time для Client Ftp;
- Объемы полученного/переданного трафика (Traffic Received/Sent) для Client E-mail и Client DB;
- загрузку, задержку, объем полученного/переданного трафика (Traffic Received/Sent) в разделе Ethernet.

4.1.7 Настройка протокола сети.

Для настройки общего для всей сети протокола переходим в пункт меню Протоколы (Protocols) - Wireless LAN - Configure PHY and Data Rate.

На диалоговом окне настроек протокола нужно выбрать стандарт беспроводной связи (Technology – 802,11g (Extended Rate PHY)) и скорость передачи беспроводной сети (54 мб/с) (Рисунок 4.17).

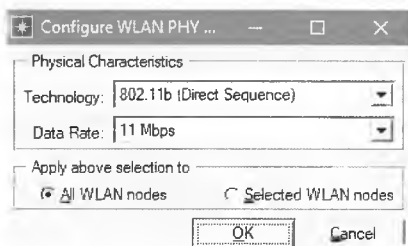


Рисунок 4.17 – Настройки протокола сети

4.1.8 Имитационное моделирование.

Теперь можно приступить к имитационному моделированию (симуляции), предварительно сохранив проект, нажав в меню проекта кнопку «Save». Проект будет по умолчанию сохранен в C:\Documents and Settings\user\op_models, но также его можно переместить и в другое место хранения данных. При повторном запуске программы OpNET для открытия существующего проекта необходимо в меню «File» выбрать «Open» и название своего проекта. Перед началом процесса симуляции необходимо

настроить некоторые параметры симуляции. Для этого на панели инструментов нужно нажать кнопку «configure/run simulation» и войти в режим симуляции (Рисунок 4.15). Пакет OpNet Modeler предлагает указать продолжительность работы сети (в данном случае – 3 часа) (Рисунок 4.18).

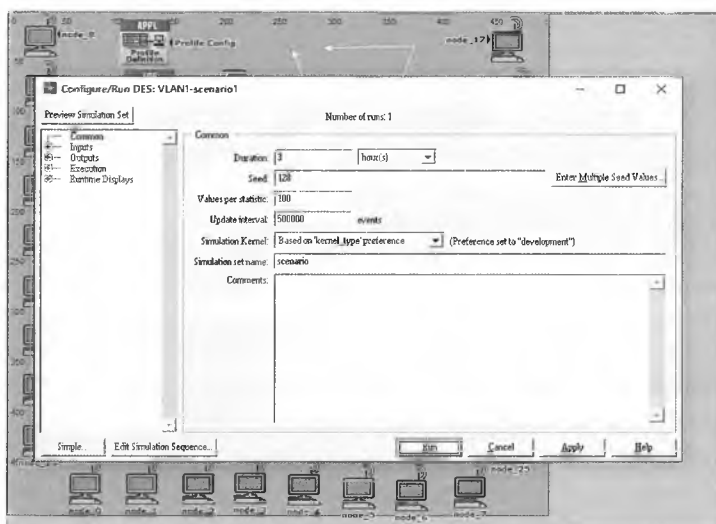


Рисунок 4.18 – Запуск симуляции

В закладках в окне симуляции имеется возможность настройки глобальных параметров сети, параметров моделирования для каждого элемента, вывода отчетов, анимации во время моделирования и др. Теперь можно запускать процесс моделирования. Чтобы запустить симуляцию нужно нажать кнопку «Run». Если вся сеть настроена корректно, то есть индивидуальные идентификаторы сети BSSID не совпадают, расставлены только нужные элементы, то симуляция завершится без предупреждений и ошибок (Рисунок 4.19).

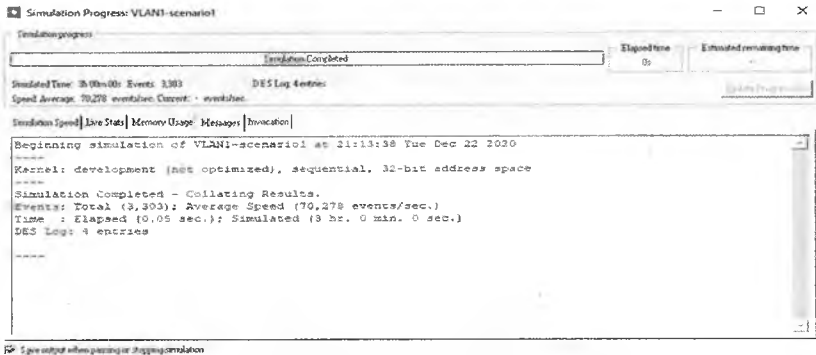


Рисунок 4.19 – Результаты Симуляции

4.1.9 Проведение атаки с использованием Wireshark.

До проведения атаки с использованием анализатора трафика Wireshark, необходимо дополнить схему, добавив в нее дополнительное устройство, представляющее из себя порт SITL. Это устройство позволяет соединить виртуальные устройства программы Ornet Modeler и реально существующее сетевое оборудование [16]. Для добавления SITL необходимо перейти в палитру устройств, Object Palette, и в рабочую область разместить устройство «sntl_virtual_gateway_to_real_world», и соединить это устройство с ранее, установленным Сервером с помощью определенного кабеля «sntl_virtual_eth_link» (Рисунок 4.20).

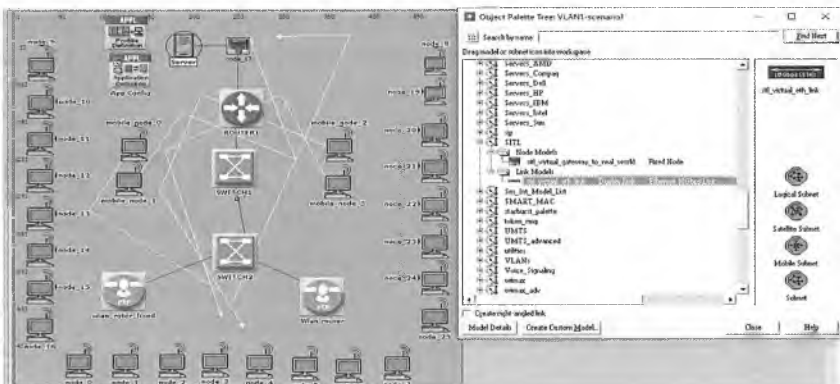


Рисунок 4.20 – Размещение и подключение дополнительного устройства SITL

После того, как устройство размещено в рабочей области, необходимо настроить новое устройство. Для этого необходимо перейти в пункт меню Добавления Атрибутов (Edit Attributes) и выбрать сетевой адаптер, который существует на используемом ПК (Рисунок 4.21).



Рисунок 4.21 – Настройка сетевого подключения

Следующим шагом дополнительной настройки сети является присвоение индивидуального адреса сети и маски подсети, для этого нужно перейти в пункте меню Сервера Добавления Атрибутов (Edit Attributes) (Рисунок 4.22).

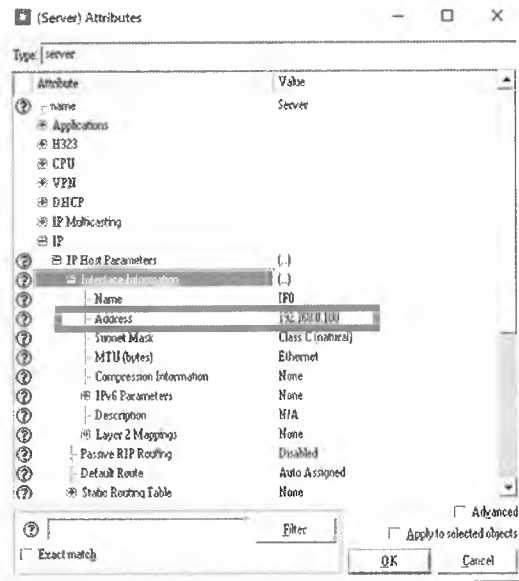


Рисунок 4.22 – Присвоение IP-адреса сервера

4.1.10 Захват сетевого трафика.

До запуска модуляции сети необходимо запустить анализатор трафика и выбрать определенное сетевое подключение, через которое будет прослушиваться трафик и которое было указано в настройках устройства SITL, затем нажимается «Старт» и начинается сбор трафика (Рисунок 4.23).

Выполнить захват трафика можно также через команду в меню Capture - Options. В открывшемся диалоговом окне устанавливаются следующие параметры захвата пакетов:

а) прописать место сохранения будущего захваченного файла в окне Capture file(s) -> File;

б) установить размер захваченного файла, поставив галочке напротив функции Use multiple files ->, выбрать размер;

в) при необходимости установить ограничение на размер захваченного файла в поле Stop Capture, ограничив по количеству пакетов, байт, минут.

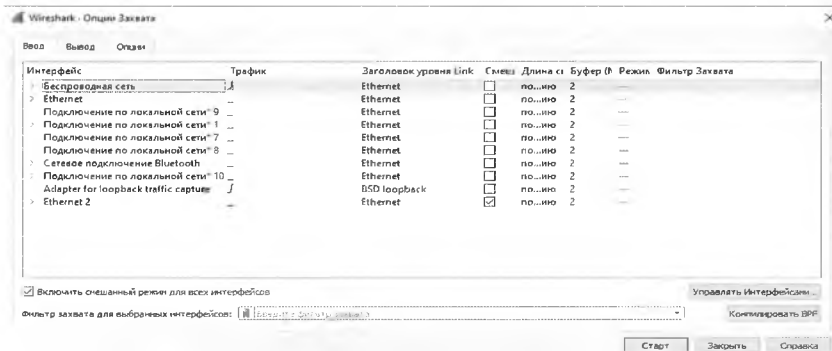


Рисунок 4.23 – Выбор сетевого интерфейса для захвата

4.1.11 Фильтрация пакетов.

После выбора интерфейса и захвата трафика выводится окно захвата пакетов (рисунок 4.24), описание полей представлено в таблице 4.2.

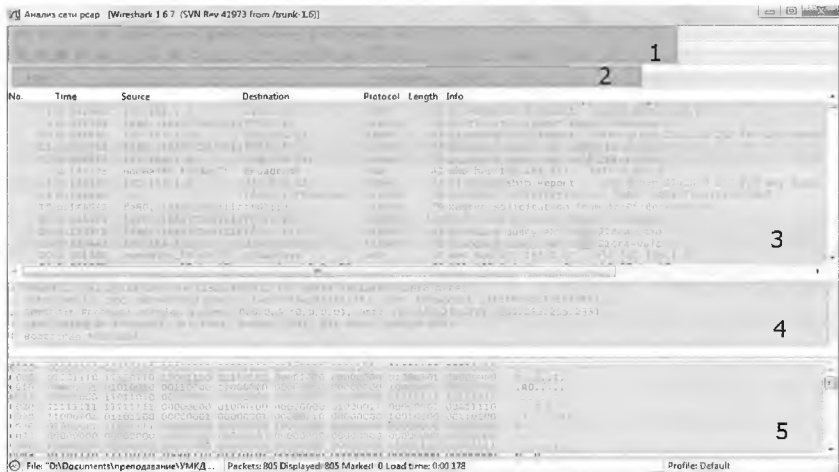


Рисунок 4.24 – Окно захваченных пакетов

Столбцы поля 3 показывают:

- No. – номер пакета в файле захвата;
- Time – временная отметка пакета;
- Source – адрес отправителя (откуда пришел пакет);
- Destination – адрес получателя (куда пакет пойдет);

- Protocol – название протокола в сокращенной версии;
- Info – дополнительная информация о содержании пакета.

Таблица 4.2 – Описание полей окна захвата

Выделенная область	Описание
1	Меню программы и панель инструментов наиболее часто используемых функций программы
2	Фильтр захваченных пакетов
3	Поле списка краткой информации по всем захваченным PDU (Packet list)
4	Информационное поле отображения подробной информации по конкретно выбранному PDU (Packet Details)
5	Поле отображения данных, выделенных в информационном поле в шестнадцатеричной и текстовой форме (Packet Bytes)

Фильтр может применяться как при захвате трафика в реальном времени, так и при его анализе, сохранённого в файле захвата.

Для применения фильтра необходимо:

- 1) Ввести фильтр в поле ввода.
- 2) Нажать кнопку «Apply».

Поле для ввода фильтра может менять цвет в зависимости от того, что было набрано.

Зеленый цвет означает, что все в порядке.

Красный – допущена ошибка.

Желтый – получен неожиданный результат, потому что существуют другие варианты написания фильтра (например, можно написать *ip.dst != 8.8.8.8* или же *!ip.dst == 8.8.8.8*, именно второй вариант более предпочтительный).

Осуществим фильтрацию по протоколам TCP (рисунок 4.25), аналогично произведем фильтрацию по протоколам HTTP, DNS.

Чтобы произвести анализ нужно отфильтровать пакеты по протоколам TCP и FTP, аналогично производится фильтрация по протоколам HTTP и DNS (рисунок 4.25).

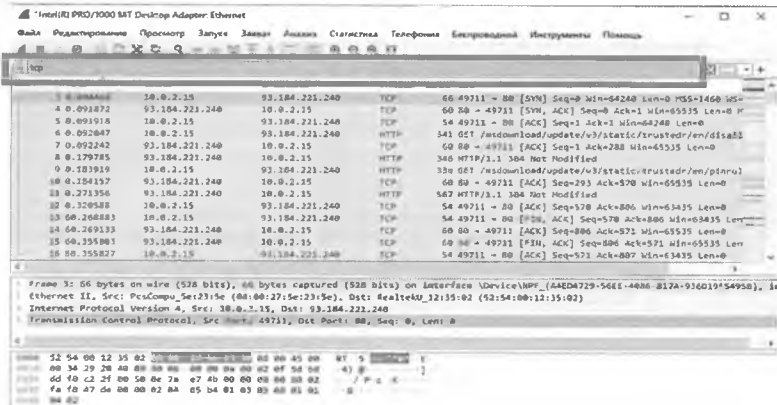


Рисунок 4.25 – Фильтрация захваченного трафика

Для извлечения файлов или картинок из захваченных файлов необходимо произвести фильтрацию по пакетам протокола HTTP.

Далее для извлечения информации перейти в меню *File – Export Objects – HTTP*. Появится окно, которое покажет все захваченные http объекты — текстовые файлы, картинки и т.д (рисунок 4.26).

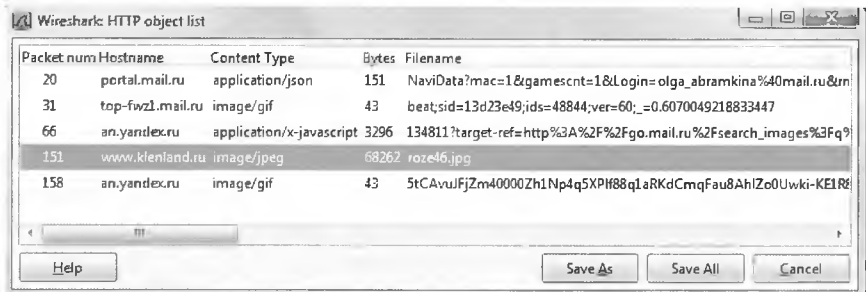


Рисунок 4.26 – Список захваченных файлов

Для того чтобы извлечь любой файл из этого списка, достаточно просто выделить его и нажать «Save As».

Рисунок был извлечен без каких-либо проблем. Таким же способом, можно извлекать и потоковое видео/аудио.

Для того чтобы быстро просмотреть передаваемые данные в рамках того или иного сеанса, используют команду меню Analyze - Follow TCP Stream. После выполнения команды на экране появится диалоговое окно, в котором разными цветами будут отображены как запросы клиента, так и ответы сервера.

Кнопка «Entire conversation» с раскрывающимся списком позволяет отобразить обе стороны, участвующие в обмене, или только одну из них. Диалоговое окно позволяет отобразить данные в различных форматах (ASCII, EBCDIC, Hex Dump, C Arrays, Raw) и сохранить их в файл. При обнаружении в сеансе кадров с каким-либо файлом можно отобразить лишь поток соответствующего направления, выбрать необходимый формат и сохранить его на диск.

Wireshark может выводит полученную информацию в графическом режиме, что облегчает ее восприятие. Перейдя в меню Statistics-Graphs tool, можно выбрать несколько фильтров для сравнения файлов позаголовочно с помощью выделения различными цветами.

Выбрав меню *Analyze-Expert Info Composite* произведем извлечение сообщений об ошибках и флаги предупреждения (такие, как потерянный или не в очереди сегмент) для быстрого обнаружения проблемы, что представлено на рисунке 4.27.

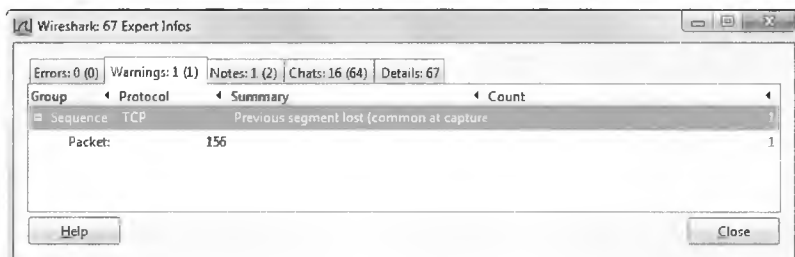


Рисунок 4.27 – Окно функций обнаружения ошибок

Описание вкладок меню и цвет, которым элементы будут отмечены в графическом интерфейсе программы:

– Chat/Чат (серый): информация об обычном рабочем процессе. Например, TCP пакет с установленным флагом SYN;

– Notes/Примечания (голубой): значительные предупреждения. Например, приложение вернуло такой код ошибки, как HTTP 404;

– Warning/Предупреждения (желтый): предупреждение, например, когда приложение вернуло такой код ошибки как «проблема связи»;

– Errors/Ошибка (красный): Серьезная проблема, например, сформированный пакет.

4.2 Проектирование глобальной беспроводной сети в программной среде Opnet Modeler v.14.5 и реализация атаки на разработанную сеть с помощью Wireshark

4.2.1 Создание архитектуры беспроводной сети в Opnet.

Для создания глобальной беспроводной сети необходимо создать проект, нажав на «File» пиктограммы Opnet. Далее, нажимая на «OK», даем наименование нашему проекту, на английском языке, например, Project_555555 и нажмем на «OK».

Далее нажимая на «OK» получим окно, из которого выберем «Create empty – scenario – Next – Enterprise – Next – Specify size – Next», далее по умолчанию нажимая «Next» до завершения стандартных настроек получаем рабочую область проекта с палеткой объектов (рисунок 4.28).

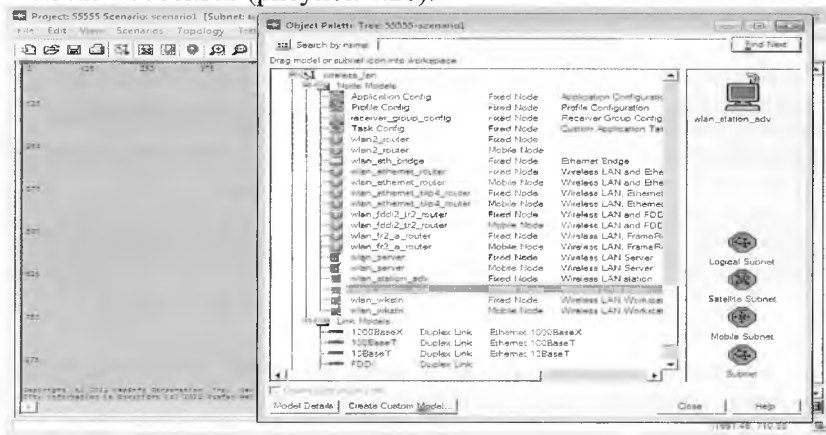


Рисунок 4.28 – Выбор технологии для использования организации своей сети

На рисунке 4.28 выбрать из приведенного окна беспроводную рабочую станцию нажатием на левой стороне wlan_station_adv в разделе wireless_lan – Node Models.

Далее выбираем необходимое оборудование для построения архитектуры глобальной беспроводной сети в соответствии с таблицей 4.3.

Таблица 4.3 – Элементы проектируемой сети

Кол-во	Компонент	База ресерсов	Описание
6	wlan_wkstn (Mobile node)	wireless_lan	Компьютеры (мобильный узел)
2	ethernet server	internet toolbox	Сервер
1	IP32_cloud	Node models	Облако интернет по протоколу IP
2	Rtr_CS_7200	Cosco (node models)	Маршрутизатор
2	wlan_ethernet_router	wireless_lan	Wireless LAN и Ethernet IP Router
4	100BaseT	internet toolbox	Соединительные линии
1	Application Config	wireless_lan	Определяет стандартные и пользовательские приложения, используемые в имитационном моделировании, включая параметры трафика и качества обслуживания
1	Profile Config	wireless_lan	Определяет режимы использования приложений пользователями группой пользователей
1	Attacker	Workstation	ПК с установленным ПО Wireshark

После выбора оборудования провести интерфейсы объемом 100 baseT в соответствии с архитектурой на рисунке 4.29.

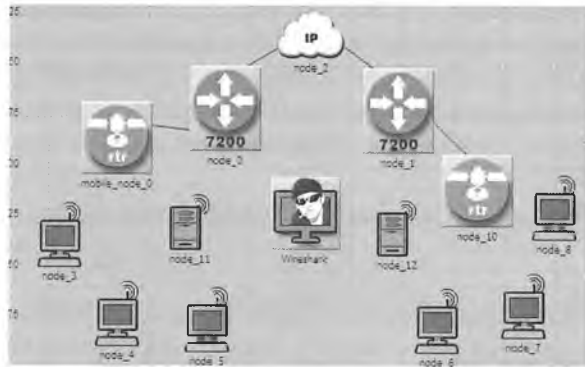


Рисунок 4.29 – Проектируема беспроводная глобальная сеть
4.2.2 Настройка оборудования сети, генерация трафика.

Необходимо провести настройки оборудования в сети, для этого нажимаем на каждом оборудовании правой кнопкой мыши и устанавливаем необходимые параметры как было показано в настройках локальной беспроводной сети. После этого нажимаем на главном меню пиктограмму Traffic и выбираем VoIP, нажимая на него, генерируем голосовой трафик, как показано на рисунках 4.30 – 4.31.

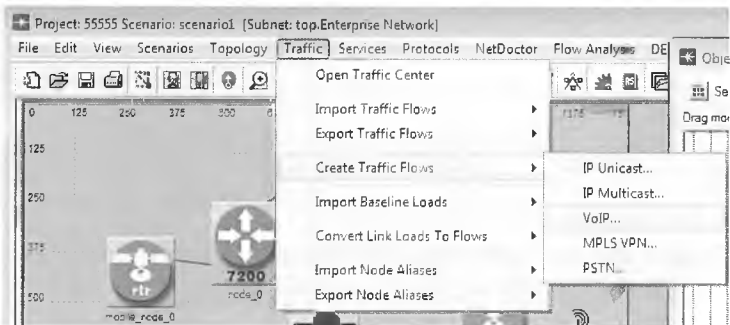


Рисунок 4.30 – Процесс выбора типа генерируемого трафика

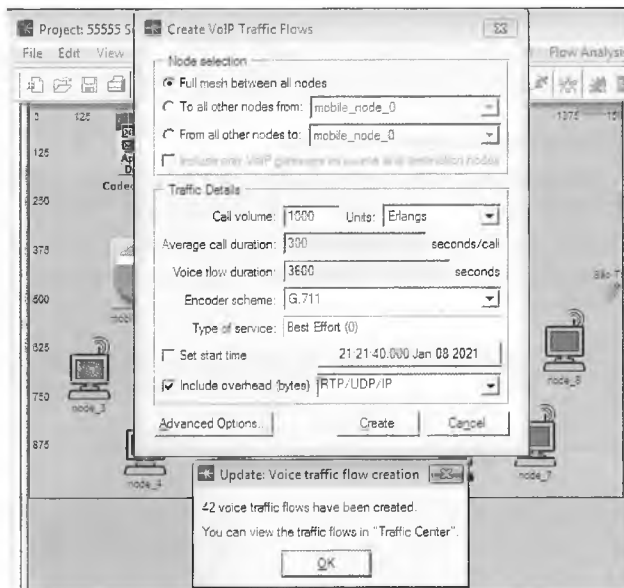


Рисунок 4.3 – Процесс генерирования голосового трафика

Нажимая на «create» получаем 42 голосовых канала. Теперь открываем на главном меню вкладку Traffic – Open traffic center и далее получаем график распределения нагрузки 42х голосовых каналов (рисунок 4.32).

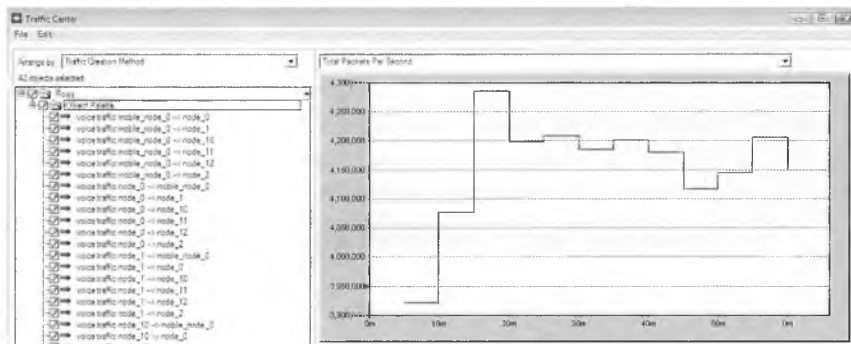


Рисунок 4.32 – Результат моделирования сети

Из рисунка 4.32 видно, что по сети проходит 4 300 000 пакетов и сеть за модельное время имеет всплески нагрузки.

4.2.3 Реализация атаки на сеть.

Для реализации атаки на проектируемую сеть необходимо запустить программу Wireshark и провести захват пакетов проходящих в сети Ornet. Для этого необходимо на программе Ornet нажать на подменю Application Capture Manager (рисунок 4.33).

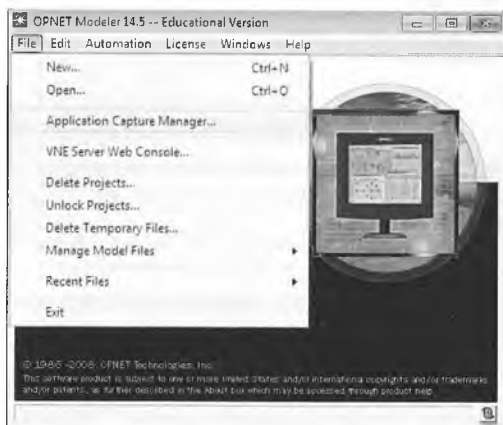


Рисунок 4.33 – Окно Application Capture Manager

После нажатия на Application Capture Manager получаем окно, в котором отражен список возможных агентов для захвата трафика (рисунок 4.34).

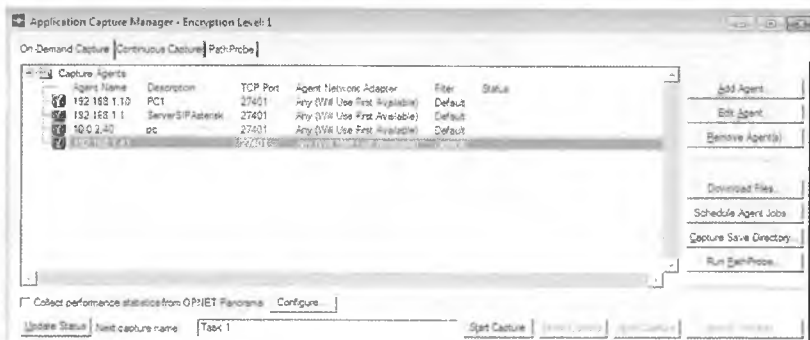


Рисунок 4.34 – Окно включения Capture Agents

Нажимая на «Add Agent» получаем следующее окно, где записываем IP адрес компьютера на котором работаем, например 192.168.1.10 (рисунок 4.35).

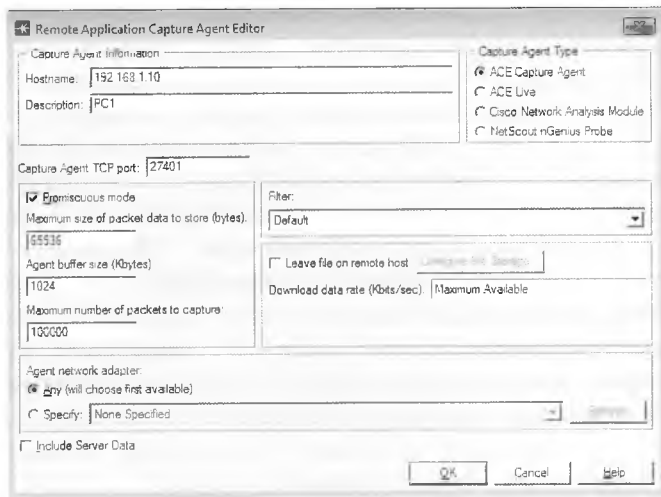


Рисунок 4.35 – Окно настройки агента

Далее нажимаем на ОК и переходим в основное окно агента, где необходимо нажать на «Start Capture» (внизу окна) для начала захвата трафика. Теперь появляется готовность связи с Wireshark после его запуска.

После открытия Wireshark появляется интерфейс программы Ornet-agent и на ней проводим процедуру захвата трафика. После, нажимая, на вкладку «Статистика» в главном меню программы Wireshark выбираем подменю график и получаем захваченные пакеты, которые приведены на рисунке 4.36.

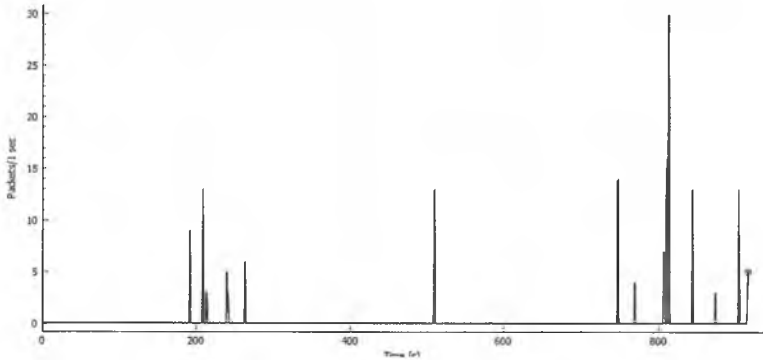


Рисунок 4.36 – Захваченный трафик wireshark

Из рисунка 4.36 видно, какова активность пакетов за захваченное время.

Также можно произвести фильтрацию на графике по разным типам протоколов, чтобы отследить сетевую активность.

Вопросы для самоконтроля:

- 1 Как осуществляется настройка интерфейсов захвата в программе Wireshark?
- 2 Что такое маршрутизатор?
- 3 Что такое коммутатор?
- 4 Как осуществить конфигурирование маршрутизаторов в среде Opnet Modeler 14.5?
- 5 Как произвести настройку приложений пользователя в среде Opnet Modeler 14.5?
- 6 Что такое протокол IP? Преимущества и недостатки протокола IP?
- 7 Как извлечь информацию из захваченных пакетов в Wireshark?
- 8 Как вывести график зависимости трафика в Wireshark?
- 9 Как осуществить фильтрацию пакетов в Wireshark?
- 10 Как произвести извлечение сообщений об ошибках в Wireshark?
- 11 Как произвести настройку протокола беспроводной сети в среде Opnet Modeler 14.5?
- 12 Как настроить движения мобильных станций по заданной траектории в среде Opnet Modeler 14.5?

Список литературы

1. Вострецова, Е.В. Основы информационной безопасности: учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург: Изд-во Урал. ун-та, 2019. - 204 с.

2. Джилкибаева А.К. Роль информационных и коммуникационных технологий в Республике Казахстан: текущее состояние, проблемы и пути совершенствования. АО «Институт экономических исследований», Астана, 2012.

3. Үмбетәлі Қ.Н. Информационная безопасность республики Казахстан. Казахская цивилизация (Университет Кайнар). Алматы. 2017. <https://articlekz.com/article/19962>

4. Махмутов А. Концепция национальной безопасности Казахстана в контексте современных внешнеполитических реалий // Материалы круглого стола «Внешиеполитические перспективы и новые концепты международной стратегии Казахстана». Институт мировой экономики и политики при Фонде Первого Президента Республики Казахстан — Лидера Нации. — 2012. — 12 марта. // iwep.kz/index

5. Постановление Правительства Республики Казахстан от 30 сентября 2011 г. № 1128 «О проекте Указа Президента Республики Казахстан «О Концепции информационной безопасности Республики Казахстан до 2016 года» (утвержден) // Электронная база нормативно-правовых актов «Параграф». online.zakon.kz/

6. Информационная безопасность. Официальный сайт Комитета национальной безопасности Республики Казахстан. knb.kz

7. Мещеряков Р.В. Основы информационной безопасности. Методические указания для выполнения практических и самостоятельных работ для студентов направления подготовки 10.03.01 и специальностей 10.05.02, 10.05.03, 10.05.04. Томск, 2017. – 66 с.

8. Стандарт ISO:17799-00 (Стандарт Великобритании BS 7799-95 "Практические правила управления ин-формационной безопасностью").

9. Вихорев С.В. Классификация угроз информационной безопасности. Терминология и подходы к классификации. "Элвис Плюс". 2001.

10. Вихорев, С. В. Как узнать – откуда напасть или откуда исходит угроза безопасности информации (окончание) / С. В. Вихорев, Р. Ю. Кобцев // Защита информации. Конфидент. – 2002. – № 3. – С. 80–84.

11. Буй П.М., Кульгавик С.Г. Методика перекрестной оценки угроз безопасности информационных систем и их уязвимостей. Вестник Белорусского Государственного Университета Транспорта: Наука И Транспорт.-№ 2 (35), 2017 – С. 40-43.

12. Абрамкина О.А. Исследование алгоритма RSA по критериям криптостойкости в среде CRYPTool 2. Международная Научно-практическая конференция, посвященная 15-ю КАУ, 11 сентября 2012, Алматы 2012.

13. Абрамкина О.А., Шкрыгунова Е.А. Криптоанализ алгоритма RSA в среде CRYPTool2. Международный научный журнал-приложение РК «Поиск», №2/2013 г, Алматы, с.119-123.

14. Абрамкина О.А. Анализ сетевого трафика с помощью программы «Wireshark»: TCP-сеансы, извлечение информации. «Научный взгляд на современное общество» сборник статей Международной научно-практической конференции. (28 апреля 2015 г, г.Уфа).-Уфа:РИО МЦИИ ОМЕГА САЙНС, 2015. С. 10-13.

15. <https://siblec.ru/telekommunikatsii/modelirovanie-setej-i-sistem-svyazi/9-programmnyj-produkt-opnet>

16. <https://ru.wikipedia.org/wiki/Wireshark>

17. <http://read.pudn.com/downloads166/ebook/760022/Introduction%20to%20SITL.pdf>

18. Opnet Modeler [Электронный ресурс] / The Application Performance Company.– Режим доступа: \www/ URL: <http://www.opnet.com>

19. Якубова М.З., Оразалиева С.К.: Моделирование анализа распределения нагрузки в беспроводных сетях на основе применения пакета прикладных программ Opnet Modeler v.14.5.//Высшая школа казахстана: научнопедагогический журнал, №3, 2018.

20. Якубова М.З., Голубева Т. Анализ и исследование информационной безопасности телекоммуникационных сетей на основе имитационного моделирования с применением различных пакетов прикладных программ. Монография.- МОН РК, НАО «Алматинский университет энергетики и связи», 2019 <https://drive.google.com/drive/u/0/my-drive>

21. Левжинский А. С.: Моделирование и визуализация беспроводных сенсорных сетей. [Электронный ресурс]. – Режим доступа:

<http://masters.donntu.org/2011/fknt/levzhinsky/diss/index.htm>

22. Васильков, А. В. Безопасность и управление доступом в информационных системах / А.В. Васильков, И.А. Васильков. - М.: Форум, 2015. - 368 с.

23. Гафнер, В. В. Информационная безопасность / В.В. Гафнер. - М.: Феникс, 2014. - 336 с.

24. Информационная безопасность открытых систем. В 2 томах. Том 1. Угрозы, уязвимости, атаки и подходы к защите / С.В. Запечников и др. - Москва: Машиностроение, 2016. - 536 с.

25. Информационная безопасность открытых систем. В 2 томах. Том 2. Средства защиты в сетях / С.В. Запечников и др. - Москва: СПб. [и др.] : Питер, 2014. - 560 с.

26. Мельников, В. П. Информационная безопасность / В.П. Мельников, С.А. Клейменов, А.М. Петраков. - М.: Academia, 2017. - 336 с.

27. Партыка, Т. Л. Информационная безопасность / Т.Л. Партыка, И.И. Попов. - М.: Форум, Инфра-М, 2016. - 368 с.

28. Степанов Е.А. Информационная безопасность и защита информации. Учебное пособие / Е.А. Степанов, И.К. Корнеев. - М.: ИНФРАМ, 2017. - 304 с.

29. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей / В.Ф. Шаньгин. - М.: Форум, Инфра-М, 2017. - 416 с.

30. Ярочкин, В. Безопасность информационных систем / В. Ярочкин. - М.: Ось-89, 2016. - 320 с.

31. Петелин А. Е. Информационная безопасность : учебнометодический комплекс : [для студентов вузов по направлению 23.07.00 "Прикладная информатика"] / А. Е. Петелин ; Том. гос. ун-т. - Томск : Томский государственный университет, 2016. URL: <http://vital.lib.tsu.ru/vital/access/manager/Repository/vtls:000534758>

32. Основы информационной безопасности <http://www.intuit.ru/studies/courses/10/10/info>

33. Основы современной криптографии: учебный курс / С.Г. Баричев, В.В. Гончаров, Р.Е. Серов.- 3-е изд. стереотип.- М.: Горячая линия-Телеком, 2011.- 175с.

34.Рябко, Б.Я. Криптографические методы защиты информации: учеб.пособие для вузов / Б.Я. Рябко, А.Н. Фионов.- 2-е изд.стереотип.- М.: Горячая линия-Телеком, 2012.- 229с.

35.Tolqin Teshabayev, Muborak Yakubova, Tuugun Nishanbaev, Bakhodir Yakubov, Tatyana Golubeva, Gulnara Sadikova. Analysis and research of capacity, latency and other characteristics of backbone multiservice networks based on simulation modeling using different routing protocols and routers from various manufacturers for using the results when designing and modernization of multiservice networks. INTERNATIONAL CONFERENCE ON INFORMATION SCIENCE AND COMMUNICATIONS TECHNOLOGIES ICISCT 2019 APPLICATIONS, TRENDS AND OPPORTUNITIES 4-6 November 2019, Tashkent Uzbekistan Tashkent University of Information Technologies named after Muhammad al-Khwarizmi TUIT.

36.Teshabayev T.Z, Yakubova M.Z., Nishanbayev T.N., Amreev M., Sadikova G.S.The formation of the structure of a multiservice network based on communication equipment from different manufacturers. INTERNATIONAL CONFERENCE ON INFORMATION SCIENCE AND COMMUNICATIONS TECHNOLOGIES ICISCT 2019 APPLICATIONS, TRENDS AND OPPORTUNITIES 4-6 November 2019, Tashkent Uzbekistan Tashkent University of Information Technologies named after Muhammad al-Khwarizmi TUIT.

37.Yakubova M.Z, Tashev K.A., Manankova O.A., Sadikova G. S.Methodology of the Determining for Pearson's Criterion based on Researching the Value of Delays in the Transmitting of Information over a Multiservice Network. 2020 International Conference on Information Science and Communications Technologies (ICISCT), Tashkent, Uzbekistan, 2020.

38.M.Amreyev, B.Yakubov, R.Safin, M.Yakubova. Improving The Quality And Reliability Of Signal Transmission And Reception In Multiservice Networks» News of Theational Academy of Sciences of the Republic of Kazakhstan. Physico-mathematical series. ISSN 1991-346X. Volume 2, Number 330 (2020), pp. 75 – 79, doi.org/10.32014/2020.2518-1726.17.

Blank lined paper with horizontal ruling lines.