ТЕОРЕТИЧЕСКИЙ МАТЕРИАЛ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

ПРОТИВОДЕЙСТВИЕ КИБЕРПРЕСТУПНОСТИ И ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

Авторы:
Д.Н. Лахтиков, начальник кафедры информационного права факультета криминальной милиции, кандидат юридических наук, доцент
П.Л. Боровик, доцент кафедры информационного права факультета криминальной милиции, кандидат юридических наук, доцент
В.И. Пикта, старший преподаватель кафедры информационного права факультета криминальной милиции

ОГЛАВЛЕНИЕ

СОКРАЩЕНИЯ И УСЛОВНЫЕ ОБОЗНАЧЕНИЯ

ВПО	Вредоносное программное обеспечение
ВТСС	Вспомогательные технические средства и системы
ЕЦП	Единая цифровая платформа Министерства внутренних дел Республики Беларусь
Информация ограниченного распространения	Информация, распространение и (или) предоставление которой ограничено, не отнесенная к государственным секретам
ИБ	Информационная безопасность
ИС	Информационная система
КЗ	Контролируемая зона
КУИ	Канал утечки информации
ЛВС	Локально-вычислительные сети
МНИ	Машинный носитель информации
МЭ	Межсетевой экран
НСД	Несанкционированный доступ
ОВД	Органы внутренних дел
ОС	Операционная система
ПО	Программное обеспечение
ПЭМИН	Побочные электромагнитные излучения и наводки
СВТ	Средство вычислительной техники
ТКУИ	Технический канал утечки информации
ТСОИ	Технические средства обработки информации
ТСПИ	Технические средства передачи информации
ЭЦП	Электронная цифровая подпись

ВВЕДЕНИЕ

Информационные технологии приобрели глобальный трансграничный характер и стали основой развития современного государства вне зависимости от территориальности, ресурсной базы, экономического, научно-технического и иных потенциалов. В настоящее время массовая информатизация и компьютеризация, привели к развитию рынка компьютеров и программного обеспечения, повышению уровня подготовки пользователей, увеличению потребностей организаций в совершенствовании технологий обработки данных, значительно расширила сферу применения информационных технологий, которые все чаще организуются в локальные сети, подключаются к сетям широкого доступа.

Изобретение, позволившее обеспечить любому человеку доступ к огромному объему информации и связавшее весь мир воедино, стало оружием и в руках преступности, возможности сети Интернет не были оставлены без внимания злоумышленников, которые используют его в своих целях. На текущем этапе уже нет сомнений, что правоохранительным органам необходимо вести активную борьбу с преступностью не только в реальном мире, но и в киберпространстве, используя Интернет как инструмент для предупреждения, выявления и пресечения преступлений.

В настоящее время актуальность противодействия киберпреступности нисколько не уменьшилась, а наоборот, только увеличилась. Распространение киберпреступлений получило существенный импульс ввиду широкой цифровизации всех сфер жизнедеятельности человека, ключевую роль играют при этом информационные технологии.

Особую актуальность приобретают вопросы правовой регламентации оборота и защиты информации. В связи со стремительным развитием в мире информационных технологий внимание и интерес к проблеме обеспечения ИБ начали существенно набирать обороты. Появились и продолжают появляться новые технологии и инструменты для сбора, хранения и обработки данных о личной жизни обычных людей и деятельности государственных органов и субъектов хозяйствования. Обеспечение ИБ способствует обеспечению

национальной безопасности, формированию информационного общества Республики Беларусь и его все более важной роли в социально-экономическом развитии Беларуси как суверенной и независимой страны, а также реализации стратегий и планов по созданию возможностей цифровой экономики и общего научно-технического прогресса.

Учебное пособие содержит положения о правовых и организационно-технических мерах обеспечения ИБ, каналах утечки информации и безопасность информационных систем, аппаратном и программном обеспечение защищенных компьютерных систем, основах противодействия киберпреступности, особенностях обнаружения, фиксации и анализа компьютерной информации.

ГЛАВА 1.

ПРАВОВЫЕ И ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИЕ МЕРЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ РЕСПУБЛИКИ БЕЛАРУСЬ

1.1. Правовое регулирование информационной безопасности

Ни одна сфера жизни современного общества не может функционировать без развитой информационной сферы. Информация и информационные коммуникации стали сегодня факторами, способными обеспечить стабильность и развитие общества и государства в целом, либо разобщить и дестабилизировать общество. Таким образом, информацию сегодня можно рассматривать как важнейший элемент системы национальной безопасности страны в целом.

Отрасль ИБ в Республике Беларусь формируется под влиянием двух основных факторов – мировых тенденций развития информационных технологий и меняющегося, в связи с этим характера киберугроз. Серьезную роль на вектор развития отрасли оказывают также изменения законодательства.

Безопасность как общенаучная категория может быть определена как состояние рассматриваемой системы, при котором последняя, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних угроз, а с другой – ее функционирование не создает угроз для элементов самой системы и внешней среды.

Национальная безопасность *определяется как состояние защищенности национальных интересов Республики Беларусь от внутренних и внешних угроз.*

Безопасность проявляется через отсутствие вреда функционированию и свойствам объекта либо его структурным составляющим. Это положение служит методологическим основанием для выделения видов безопасности, в частности ИБ. Одна из важных структурных составляющих выделенных объектов безопасности – информация или деятельность, предметом которой является информация. Наличие угроз этим объектам (интересам государства, общества, личности) позволяет говорить об их ИБ – безопасности объектов, относящихся и входящих в область этих интересов, и необходимости защиты информации.

В соответствии с действующим законодательством ***информационная безопасность*** *– это состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере*.

ИБ государства заключается в невозможности нанесения вреда его деятельности по выполнению функций управления делами общества, связанных с использованием информации и информационной инфраструктуры.

Информационная коммуникация осуществляется посредством среды распространения информации, принимающей в современном обществе форму информационной инфраструктуры. Нанесение вреда этой инфраструктуре, передаваемым сообщениям и содержащимся в них сведениям может привести к нарушению информационной коммуникации и, как следствие, к разрушению целостности общества, дестабилизации деятельности его институтов.

ИБ общества также заключается в невозможности нанесения вреда его духовной сфере, культурным ценностям, социальным регуляторам поведения людей, информационной инфраструктуре и передаваемым с се помощью сообщениям.

ИБ личности состоит в невозможности нанесения вреда человеку как личности, социальная деятельность которой во многом базируется на осмыслении получаемой информации, информационных взаимодействиях с другими индивидами и которая часто использует информацию в качестве предмета деятельности.

Составляющими ИБ, ее компонентами, в совокупности будут:

объекты ИБ,

угрозы объектам ИБ,

политика обеспечения ИБ,

система обеспечения ИБ.

Приведенная модель ИБ является применимой на различных организационных уровнях обеспечения ИБ:

государственном уровне (уровне Республики Беларусь),

уровне государственного органа (организации, предприятия, учреждения),

уровне технической системы обработки, хранения и передачи информации.

Для каждого из указанных уровней к настоящему времени сложились достаточно полные научные знания и соответствующая практика обеспечения ИБ.

Проникая во все сферы деятельности государства, информация приобретает конкретное материальное, социальное, политическое и стоимостное выражение. На этом фоне все более актуальный характер приобретают вопросы обеспечения ИБ Республики Беларусь как неотъемлемого элемента национальной безопасности, а защита информации, в том числе информационных ресурсов, продуктов, услуг и информационно-технического комплекса средств их обработки превращается в одну из приоритетных государственных задач.

Информация является основным средством взаимодействия человека с другими людьми, без которого решение перечисленных задач не представляется возможным. Посредством информации осуществляется процесс воспитания, образования, с ее помощью происходит овладение трудовыми навыками, формируется представление человека о возможных способах удовлетворения нужд, потребностей и реализации интересов, осуществляются мотивация его деятельности, а также в определенной мере и сама деятельность.

Нанесение вреда информации, способности человека ее формировать, воспринимать и осмысливать чревато негативными последствиями для

человека как социального и биологического существа, снижает возможность его выживания в реальном мире.

Поэтому важнейшим понятием в этой связи является ***защита информации***, которая представляет собой *комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации.*

В соответствии с Концепцией ИБ Республики защищенность информации достигается комплексом мер, реализуемых функционированием системы обеспечения ИБ.

В свою очередь, ***система обеспечения ИБ*** *является совокупностью правовых, организационных и технических мероприятий, средств и методов защиты, органов управления и исполнителей, направленных на противодействие угрозам ИБ с целью предотвращения либо существенного затруднения утечки, хищения, утраты, уничтожения, искажения, модификации, подделки, копирования, блокирования информации и несанкционированного доступа к ней.*

Целями правового регулирования в области обеспечения ИБ является достижение конфиденциальности, целостности и доступности в информационной сфере. Данные цели отличают ИБ от иных видов безопасности и определяют направленность соответствующего правового регулирования. Одно из важнейших направлений работы по построению безопасности в информационной среде – совершенствование нормативной правовой базы в зависимости от возникающих современных вызовов.

Конституционные основы, с которыми можно связать ИБ, заложены в ст. 28 Конституции Республики Беларусь, гарантирующей право на защиту гражданина от незаконного вмешательства в его личную жизнь, в том числе от посягательства на тайну его корреспонденции, телефонных и иных сообщений, на его честь и достоинство. В свою очередь, в ст. 34 Конституции Республики Беларусь указывается, что пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав.

Кроме того, ст. 59 Конституции определяет, что государство обязано принимать все доступные ему меры для создания внутреннего и международного порядка, необходимого для полного осуществления прав и свобод граждан Республики Беларусь, предусмотренных Конституцией. Государственные органы, должностные и иные лица, которым доверено исполнение государственных функций, обязаны в пределах своей компетенции принимать необходимые меры для осуществления и защиты прав и свобод личности.

В соответствии с приведенными и иными основополагающими нормами Конституции в Республике Беларусь разработан и осуществляется комплекс правовых и организационно-практических мер, направленных на обеспечение ИБ. Помимо Конституции Республики Беларусь, существует ряд иных нормативных правовых актов, которые призваны обеспечить ИБ, например:

Закон Республики Беларусь от 10.11.2008 г. № 455-З «Об информации, информатизации и защите информации»;

Закон Республики Беларусь 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»;

Закон Республики Беларусь от 07.05.2021 № 99-З «О защите персональных данных»;

Указ Президента Республики Беларусь от 01.02.2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет»;

Указ Президента Республики Беларусь от 25.10.2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации»;

Указ Президента Республики Беларусь от 16.04.2013 г. № 196 «О некоторых мерах по совершенствованию защиты информации»;

Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности»;

Постановление Совета Министров Республики Беларусь от 15.05.2013 г. № 375 «Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. ИБ» (ТР 2013/027/BY)»;

Приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 28.03.2014 № 26 «О порядке размещения программно-технических средств, информационных систем (ресурсов) на ресурсах республиканского центра обработки данных и (или) республиканской платформы» (вместе с «Положением о порядке размещения программно-технических средств, информационных систем (ресурсов) государственных организаций на ресурсах республиканского центра обработки данных и (или) республиканской платформы»);

Постановление Оперативно-аналитического центра при Президенте Республики Беларусь, Комитета государственной безопасности Республики Беларусь и Министерства связи и информатизации Республики Беларусь от 27.12.2022 г. № 6/24/25 «О порядке ограничения (возобновления) доступа к интернет-ресурсу поставщика услуг электросвязи, владельца интернет-ресурса»;

Постановление Оперативно-аналитического центра при Президенте Республики Беларусь и Комитета государственной безопасности Республики Беларусь от 10 января 2023 г. № 1/1 «О технических требованиях».

Постановлением Совета Безопасности Республики Беларусь от 18.03.2019 г. № 1 «О Концепции ИБ Республики Беларусь» определена ***цель государственной политики в области обеспечения ИБ*** *– это достижение и поддержание такого уровня защищенности информационной сферы, который обеспечивает реализацию национальных интересов Республики Беларусь и ее прогрессивное развитие.*

Концепция ИБ Республики Беларусь позволяет:

обеспечить дальнейшее формирование официальной системы взглядов на вопросы ИБ на текущем этапе общественного развития;

закрепить основные направления, формы и методы обеспечения ИБ, развивать их и дополнять по мере генерирования новых знаний и технологий;

всесторонне информировать общество о вопросах обеспечения ИБ, эффективности и обусловленности национальной политики в этом отношении, а также обеспечить постепенное доведение общего мнения Республики Беларусь по этим вопросам до международного сообщества;

консолидировать усилия государства и общества, направленные на повышение эффективности защиты национальных интересов в информационной сфере в условиях глобальной информатизации и возникновения новых угроз ИБ;

обеспечить целенаправленную и неуклонную интеграцию Беларуси в системы обеспечения международной ИБ на основе национальных приоритетов.

Особую роль среди нормативных правовых актов, регулирующих вопросы защиты информации играет Закон Республики Беларусь «Об информации, информатизации и защите информации», который определяет порядок государственного регулирования и управления в сфере защиты информации. Устанавливает механизмы защиты информации, которые конкретизируют и раскрывают иные законодательные акты. На государственном уровне осуществляются мониторинг, анализ и оценка состояния ИБ, применяются индикаторы оценки ее состояния. Определяются приоритетные направления предотвращения угроз ИБ, минимизации их деструктивного воздействия и локализации последствий.

В данном законе также определены отдельные термины и закреплены их определения:

информация *– сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;*

доступ к информации *– возможность получения информации и пользования ею;*

защита информации *– комплекс правовых, организационных и технических мер, направленных на обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;*

конфиденциальность информации *– требование не допускать распространения и (или) предоставления информации без согласия ее обладателя или иного основания, предусмотренного законодательными актами.*

Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи» определяет государственное регулирование в сфере

обращения электронных документов и электронной цифровой подписи. Так, электронная цифровая подпись предназначена для удостоверения информации, составляющей общую часть электронного документа; подтверждения целостности и подлинности электронного документа; подписания электронной копии документа на бумажном носителе. Удостоверение информации, составляющей общую часть электронного документа, осуществляется путем применения сертифицированных средств электронной цифровой подписи с использованием личных ключей (последовательность символов, принадлежащая определенным организации или физическому лицу и используемая при выработке электронной цифровой подписи) организации или физического лица (лиц), подписывающих этот электронный документ.

Закон Республики Беларусь «Об электросвязи» определяет правовые и организационные основы деятельности в области электросвязи. Нормы Закона направлены на обеспечение создания, устойчивого и эффективного функционирования и развития сетей электросвязи, на создание условий для удовлетворения нужд в услугах электросвязи физических и юридических лиц, государственного управления, национальной безопасности, обороны, охраны правопорядка, предупреждения и ликвидации чрезвычайных ситуаций.

Указом Президента Республики Беларусь от 9 апреля 2020 г. № 122 определена национальная система медиаизмерений, соответствующая мировым стандартам, закреплены основные принципы ее государственного регулирования и функционирования.

К особенностям в области использования национального сегмента интернета относится регламентация функционирования общегосударственной автоматизированной информационной системы (ОАИС), которая согласно Указу Президента Республики Беларусь от 16 декабря 2019 г. № 460 «Об общегосударственной автоматизированной информационной системе» предназначена для обеспечения эффективного электронного информационного взаимодействия в автоматическом и (или) автоматизированном режимах государственных организаций между собой, а также с иными организациями, нотариусами и гражданами посредством защищенной информационно-коммуникационной инфраструктуры.

Кроме того, Указом Президента Республики Беларусь от 23.01.2014 № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий» закреплены основы использовании государственными органами и иными государственными организациями телекоммуникационных технологий и их перехода на использование технологий облачных вычислений.

Указ Президента Республики Беларусь от 9.12.2019 г. № 449 «О совершенствовании государственного регулирования в области защиты информации», которым скорректирован порядок отнесения объектов инфраструктуры, функционирующих с использованием информационно-коммуникационных технологий, к категории критически важных объектов информатизации (КВОИ). Им также утверждены Положение о порядке отнесения объектов информатизации к КВОИ и Положение о технической и криптографической защите информации.

Также, непосредственно правового регулирования вопросов информационной безопасности касается и Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности», где определены задачи национальной системы обеспечения кибербезопасности. Также в целях повышения уровня защиты национальной информационной инфраструктуры от внешних и внутренних угроз определено создание в Республике Беларусь национальной системы обеспечения кибербезопасности. Ее элементами определены:

ОАЦ при Президенте Республики Беларусь, как государственный орган, осуществляющий координацию деятельности заинтересованных в этих вопросах;

Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты (далее – Национальный центр кибербезопасности);

а также ряд других органов и организаций.

Определено, что ОАЦ взаимодействует с иностранными и международными организациями по вопросам реагирования на киберинциденты, в том числе в рамках участия в форуме команд реагирования на компьютерные инциденты (FIRST), с уплатой взносов, связанных с таким

участием. В составе Национального центра кибербезопасности для реализации функции реагирования на киберинциденты создана национальная команда реагирования на киберинциденты (CERT.BY).

Указом определены **объекты информационной инфраструктуры**:

критически важные объекты информатизации,

информационные сети,

информационные системы,

информационные ресурсы и

иные совокупности технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации, за исключением объектов информатизации, предназначенных для обработки информации, содержащей государственные секреты.

Также закреплены понятия, которым даны определения, например:

Информационная инфраструктура *– это совокупность технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации.*

Кибератака *– это целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.*

Киберинцидент *– это событие, которое фактически или потенциально угрожает конфиденциальности, целостности, подлинности, доступности и сохранности информации, а также представляет собой нарушение (угрозу нарушения) политики безопасности.*

Касаясь необходимости защиты информации, разрабатываются различные методы защиты информации, под которыми понимаются технологии, программное обеспечение, аппаратные средства и программные средства, предназначенные для защиты информации, а также средства контроля ее безопасности и эффективности. В законодательстве особое внимание уделяется технологиям и методам шифрования для защиты информации.

Криптографическая защита информации *– деятельность, направленная на обеспечение конфиденциальности, контроля целостности и подлинности информации с использованием средств криптографической защиты информации (технические, программные, программно-аппаратные средства защиты информации, реализующие один или несколько криптографических алгоритмов (шифрование, выработка и проверка электронной цифровой подписи, хэширование, имитозащита) и криптографические протоколы, а также функции управления криптографическими ключами, механизмы идентификации и аутентификации).*

В свою очередь, ***техническая защита информации*** *– это деятельность, направленная на обеспечение конфиденциальности, целостности, доступности и сохранности информации техническими мерами без применения средств криптографической защиты информации.*

На выпускаемые в обращение на территории Республики Беларусь средства защиты информации независимо от страны происхождения, за исключением средств шифрованной, других видов специальной связи и криптографических средств защиты государственных секретов, распространяется действие технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. ИБ» (ТР 2013/027/ BY), утвержденного постановлением Совета Министров Республики Беларусь от 15 мая 2013 г. № 375.

Постановлением Совета Министров Республики Беларусь от 2 февраля 2021 года № 66 «О Государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы» утверждена указанная программа, определены ее цель, задачи и структура, подпрограммы, основные риски при выполнении государственной программы, механизмы управления рисками, методика оценки эффективности реализации государственной программы, комплекс ее мероприятий и иные важные моменты по ее реализации.

Приказ ОАЦ при Президенте Республики Беларусь от 28 марта 2014 г. № 26 «О порядке размещения программно-технических средств, информационных систем (ресурсов) на ресурсах республиканского центра обработки данных и

(или) республиканской платформы», которым утверждено Положение о порядке размещения программно-технических средств, информационных систем (ресурсов) государственных организаций на ресурсах республиканского центра обработки данных и (или) республиканской платформы. Данным Положением определяется порядок размещения существующих, создаваемых (приобретаемых, модернизируемых) программно-технических средств, информационных систем (ресурсов) государственных организаций на ресурсах республиканского центра обработки данных и (или) республиканской платформы, правовые основы использования, включающие обеспечение защиты информации на республиканской платформе;

Приказом ОАЦ при Президенте Республики Беларусь от 12.07.2016 г. № 55 «О системе противодействия нарушениям порядка пропуска трафика на сетях электросвязи» определен порядок функционирования системы противодействия нарушениям порядка пропуска трафика на сетях электросвязи, в том числе перечень информационных ресурсов являющихся неотъемлемой частью системы, порядок их создания, ведения и использования; порядок создания и внедрения комплекса технического противодействия, а также интеграции с этим комплексом программно-технических средств информационных сетей систем и ресурсов определенных операторов электросвязи и иных заинтересованных; порядок информационного взаимодействия лиц, осуществляющих деятельность по предупреждению, выявлению и пресечению нарушений порядка пропуска трафика, их права и обязанности; регламентировал ряд иных важных вопросов.

Приказ ОАЦ при Президенте Республики Беларусь от 30 сентября 2016 г. № 70 «О внесении изменений в приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 27 мая 2013 г. № 33», в редакции которого отражена Инструкция о порядке взаимодействия ведомственных систем электронного документооборота с системой межведомственного электронного документооборота государственных органов. Согласно данному приказу основной целью взаимодействия систем является обеспечение межведомственного информационного взаимодействия государственных органов на основе унифицированных информационных технологий, форматов и

протоколов обмена данных, правил и процедур их совершенствования во исполнение задач: создания эффективной системы межведомственного информационного взаимодействия государственных органов; обеспечения оперативного обмена электронными документами; минимизации финансовых и временных затрат при обмене информацией.

Приказом ОАЦ при Президенте Республики Беларусь от 12 ноября 2021 г. № 195 «О технической и криптографической защите персональных данных» определен минимальный перечень применяемых мер по защите персональных данных:

аутентификация и идентификация; антивирусная защита (регулярное обновление);

разграничение прав пользователей;

установление правил генерации и смены паролей;

установление правил работы со съемными носителями;

мониторинг (просмотр, анализ) событий информационной безопасности.

Приказом ОАЦ при Президенте Республики Беларусь от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента РБ от 09.12.2019 № 449» утверждены:

Положение о порядке технической и криптографической защиты информации в информационных системах, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;

Положением о порядке аттестации систем защиты информации информационных систем, предназначенных для обработки информации, распространение и (или) предоставление которой ограничено;

Положением о порядке технической и криптографической защиты информации, обрабатываемой на критически важных объектах информатизации;

Положением о порядке представления в ОАЦ при Президенте Республики Беларусь сведений о событиях информационной безопасности, состоянии технической и криптографической защиты информации;

Положение о порядке ведения Государственного реестра критически важных объектов информатизации.

В Республике Беларусь обеспечение безопасности в информационной сфере также осуществляется посредством правовых норм, содержащихся в уголовном и административном законодательствах.

Так, Кодексом Республики Беларусь об административных правонарушениях определены административно-правовые санкции за правонарушения в информационной сфере. Содержится глава «Административные правонарушения в области связи и информации», включающая составы административных правонарушений, предусмотренные ст.ст. 23.1-23.10, к таким правонарушениям относятся: несанкционированный доступ к компьютерной информации (статья 23.4), разглашение коммерческой или иной охраняемой законом тайны (статья 23.6), нарушение законодательства о защите персональных данных (статья 23.7), разглашение служебной тайны по неосторожности (статья 23.8).

Очевидно, что одной из наиболее эффективных мер профилактики преступлений и иных правонарушений является реализация принципа неотвратимости ответственности. Безусловно важнейшим правовым инструментом в вопросах защиты информации являются нормы Уголовного кодекса, которые имеют предупредительное значение ввиду самого факта установления уголовной ответственности за конкретные общественно опасные деяния, но важно и обеспечение неотвратимости при их нарушении. Уголовный кодекс Республики Беларусь закрепляет ответственность за преступления против компьютерной безопасности (глава 31), а также иные составы преступлений в информационной сфере (хищение путем модификации компьютерной информации (статья 212), умышленное разглашение государственной тайны (статья 373), разглашение государственной тайны по неосторожности (статья 374), умышленное разглашение служебной тайны (статья 375), незаконный оборот средств платежа и (или) инструментов (статья 222).

Таким образом, среди нормативных правовых актов можно выделить основные группы нормативных правовых актов:

о защите информации;

о доступе граждан к информации;

о компетенции органов государственной власти в сфере защиты информации.

Сложность и разнообразие используемого сетевого программного и аппаратного обеспечения, а также быстрое развитие информационных технологий и рост киберпреступности увеличили риск нестабильности ИБ. В связи с этим правовые положения о защите информации стали чрезвычайно важными и нуждаются в постоянном совершенствовании. Однако в некоторых случаях развитие правовой системы отстает от формирующихся общественных отношений, что подтверждается, когда формирование национальной политики в области ИБ происходит довольно поздно. Необходимо обеспечить одновременную, и самое главное, своевременную интеграцию правовых, организационных, технических и других мер.

Сфера ИБ Республики Беларусь нуждается в регулярном анализе защищенности, своевременном реагировании и адекватном принятии мер по устранению обнаруженных внешних и внутренних угроз безопасности, прогнозированию последствий, а также мер по предотвращению возможности негативного влияния на информационную сферу.

1.2. Организационно-технические меры обеспечения ИБ

Организационно-технические меры безопасности имеют решающее значение для обеспечения ИБ и реализуются по нескольким направлениям.

Использование технологий защиты. Целесообразно активно внедрять и использовать технологии, направленные на обеспечение защиты информации, например, такие как шифрование, антивирусное программное обеспечение, брандмауэры, системы обнаружения и предотвращения вторжений, а также виртуальные частные сети для защиты информационных систем и сетей.

Безопасность персонала. Допуск персонала, работающего с информацией, ограниченной для распространения (государственные секреты, для служебного пользования и др.). Реализация образовательных программ для повышения осведомленности о рисках и угрозах ИБ и передовых методах противодействия им.

Физическая безопасность. Физический доступ к информационной инфраструктуре (сети, системы, объекты) должен быть ограничен, контролироваться с помощью систем видеонаблюдения, возможно применение различных видов аутентификации (например, биометрической). Сюда же включаются мероприятия по реагирование на инциденты и планированию аварийного восстановления в случае инцидента безопасности или стихийного бедствия.

К мерам организационного обеспечение также можно отнести:

разработку и внедрение внутренних политик и процедур по защите информации;

заключение договоров с поставщиками услуг об обеспечении защиты информации;

обучение и повышение осведомленности сотрудников в сфере ИБ;

проведение периодических аудитов и оценок угроз ИБ;

регулярный мониторинг и оценка эффективности принятых мер и внесение необходимых корректировок.

В Республике Беларусь важное значение в сфере обеспечения ИБ отводится Оперативно-аналитическому центру при Президенте Республики

Беларусь, который был создан 21 апреля 2008 г. на базе государственного центра безопасности информации при Министерстве обороны Республики Беларусь. ОАЦ является государственным органом, ответственным за контроль деятельности по обеспечению защиты информации, содержащей государственные секреты Республики Беларусь, или иной информации, защищенной в соответствии с законодательством, на технических каналах от несанкционированной и случайной утечки. Это проявляется в разработке и учете средств защиты информации, осуществлении научно-технической деятельности, проверке, экспертизе, сертификации и выдаче лицензий на техническую и парольную защиту информации для осуществления деятельности в области защиты информации. Данный государственный орган наделён полномочиями в создании нормативных правовых актов, которые обязательны к выполнению всеми субъектами Республики Беларусь в области защиты информации.

В системе ОВД, в структуре криминальной милиции, созданы и функционируют подразделения по противодействию киберпреступности, которые выявляя и пресекая преступления против компьютерной безопасности и другие преступления, совершаемые с использованием информационно-коммуникационных технологий, оказывает существенное влияние на обеспечение национальной безопасности в информационной сфере. Также в системе ОВД функционируют подразделения по обеспечению ИБ в ведомстве и всех подчиненных структурах.

В свою очередь в Республике Беларусь функционирует ФинЦерт Национального банка Республики Беларусь, т.е. центр мониторинга и реагирования на угрозы информационной безопасности в банковской сфере, который призван осуществлять выявление и нейтрализацию киберугроз и оперативный обмен информацией между заинтересованными субъектами с целью их предупреждения или минимизации последствий.

Рассматривая созданные правовые и организационные средства обеспечения ИБ в Республике Беларусь, можно сделать вывод о том, что в настоящее время в Республике Беларусь создана достаточно эффективная

система ИБ, которая способная противостоять киберпреступности на должном уровне.

В свою очередь в ОВД разработан комплекс мер по обеспечению ведомственной ИБ, также утверждена политика ИБ единой цифровой платформы Министерства внутренних дел (далее – ЕЦП МВД), устанавливающая совокупность правил, требований и руководящих принципов в области ИБ, обязательных для исполнения сотрудниками; отражены вопросы, касающиеся защиты информации, парольной политики, защиты от вредоносного программного обеспечения и др.

Основными целями указанной Политики являются:

защита активов единой цифровой МВД от случайного или преднамеренного воздействия на информацию, носители информации, процессы обработки и передачи с целью исключения возможного нанесения ущерба или уменьшения результатов его воздействия.

обеспечение конфиденциальности, целостности, подлинности, доступности и сохранности информации;

снижение уровня рисков, связанных с ИБ;

формирование и регламентирование единых подходов и требований по обеспечению ИБ сотрудниками, а также государственными органами и организациями, иными юридическими лицами в рамках информационного взаимодействия с МВД и др.

Задачами указанной Политики являются:

определение ответственности и обязанностей участников информационных отношений по обеспечению и соблюдению требований данной Политики, в том числе с использованием программных, программно-аппаратных средств технической защиты информации;

планирование, реализация и контроль эффективности использования защитных мер и средств защиты информации, создание механизма оперативного реагирования на угрозы ИБ;

своевременное выявление и оценка источников и характера угроз ИБ, причин и условий, способствующих нанесению ущерба субъектам информационных отношений, нарушению нормального функционирования

систем МВД, и дальнейшее прогнозирование развития событий на основе мониторинга инцидентов ИБ;

создание условий для минимизации и локализации наносимого ущерба неправомерными действиями, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;

защита от вмешательства в процесс функционирования ЕЦП МВД посторонних лиц;

разграничение и обеспечение доступа пользователей к ИС в соответствии с их должностными обязанностями;

защита от несанкционированной модификации информации, хранящейся и обрабатываемой в ИС ЕЦП МВД, от внедрения несанкционированных программ, в том числе вредоносных, и устройств в ЕЦП МВД;

ЗИ от утечки при ее обработке, хранении и передаче по техническим каналам связи и др.

Обеспечение ИБ ЕЦП МВД реализуется следующими организационными и техническими мерами:

идентификация и аутентификация пользователей различных субъектов информационных отношений при обеспечении ИБ ЕЦП МВД;

управление доступом к активам;

сбор и мониторинг (просмотр, анализ) событий ИБ;

реагирование на инциденты ИБ и управление ими;

защита от вредоносного программного обеспечения;

управление информационными потоками и обеспечение сетевой безопасности;

управление процедурами резервного копирования;

обнаружение утечек защищаемой информации;

регламентация и контроль использования носителей информации, мобильных технических средств, ведомственной электронной почты;

взаимодействие с государственными органами и организациями по вопросам обеспечения ИБ;

осуществление проверочных мероприятий с целью выявления недостатков в системе ИБ МВД и др.

Объектами защиты системы ИБ ЕЦП МВД являются:

информация, хранящаяся и обрабатываемая в ИС ЕЦП МВД в соответствии с отнесенным к классам типовых ИС;

ИС, содержащие информацию, распространение и (или) предоставление которой ограничено.

Также определены обязанности пользователей ведомственной сети передачи данных (далее – ВСПД):

сообщать администратору ИС об отказах в работе ВСПД;

не допускать использование без получения соответствующего разрешения своего автоматизированного рабочего места (далее – АРМ) другими пользователями, а в случае обнаружения факта такого использования – немедленно сообщать своему непосредственному начальнику, а если указанный факт происходит с его ведома – вышестоящему руководителю;

сохранять в тайне личный пароль доступа к АРМ, подключенному к ВСПД, и не сообщать его другим лицам;

вводить личный пароль и другие учетные данные, убедившись, что клавиатура находится вне поля зрения других лиц;

немедленно заменить пароль, если он был скомпрометирован;

при оставлении без присмотра включенного АРМ ограничивать его использование посторонними лицами (путем временной блокировки экрана, клавиатуры и так далее);

не использовать АРМ в сети без установленного антивирусного обеспечения, определяемого в соответствии с законодательством Республики Беларусь в области защиты информации;

проверять на наличие вредоносного программного обеспечения внешние носители информации;

проводить антивирусный контроль с помощью антивирусных средств защиты, а в случае предупреждающего сообщения – немедленно прекратить работу и сообщить в подразделение информационных технологий (далее – подразделение ИТ);

немедленно ставить в известность сотрудников подразделения ИТ о ненадлежащей работе программного обеспечения, АРМ или ВСПД.

Кроме того, пользователю ВСПД запрещается:

фиксировать свои учетные данные (пароли, логины и иное) в бумажной, электронной формах или другом виде в общедоступных местах;

использовать ВСПД в целях, противоречащих законодательству Республики Беларусь или не связанных с выполнением служебных обязанностей;

использовать чужой логин для авторизации;

просматривать, изменять и копировать служебную и иную информацию других пользователей кроме случаев, если эти действия санкционированы;

устанавливать и запускать на АРМ программное обеспечение без утвержденного начальником структурного подразделения ОВД и согласованного с подразделением ИТ списка программного обеспечения либо без письменного разрешения начальника структурного подразделения ОВД на самостоятельную установку необходимого программного обеспечения и его удаление, согласованного с подразделением ИТ;

удалять установленное другими пользователями программное обеспечение;

осуществлять перенастройку любого программного обеспечения (в том числе операционных систем) путем изменения файлов настройки или иным образом, влияющую на работоспособность ВСПД, без согласования с подразделением ИТ;

самовольно модернизировать, заменять средства телекоммуникации, подключать к ВСПД и АРМ любые каналообразующие и коммутационные средства связи и автоматизации, в том числе мобильные телефоны, а также вносить изменения в конструкцию АРМ и других узлов ВСПД;

копировать, обрабатывать и хранить на АРМ неслужебную информацию;

подключаться к информационным ресурсам ОВД, если это противоречит установленным требованиям;

умышленно использовать недокументированные свойства и ошибки программного обеспечения или настройки ВСПД, которые могут привести к возникновению неправильной работы или к угрозе безопасности ВСПД; при

обнаружении таких ошибок пользователь обязан проинформировать начальника своего структурного подразделения и администратора.

Необходимо помнить, что соблюдение мер ИБ в повседневной деятельности сотрудника ОВД подразумевает выполнение соответствующих требований не только в служебное время, но и в нерабочее, в быту. Особое значение данная проблема приобретает в связи с активным использованием в повседневной деятельности различных информационно-коммуникационных технологий (интернет, электронная почта, социальные сети, мессенджеры, облачные хранилища и др.). С одной стороны, указанные технологии предоставляют разнообразные возможности для удобной обработки, хранения, восприятия и передачи информации. С другой стороны, они обладают широким спектром различного рода уязвимостей, существенно снижающих уровень ИБ их пользователя.

В этой связи, практические рекомендации по обеспечению ИБ сотрудника в повседневной деятельности и в быту можно представить в виде совокупности следующих мероприятий:

Безопасность электронной почты (E-mail):

подключить двухфакторную аутентификацию;

использовать надежный пароль для доступа к E-mail; использовать спам-фильтры;

использовать как минимум два типа отдельных e-mail адресов: закрытые (только для интернет-банкинга, привязки устройств и средств защиты и т. д.), открытые (только для переписки, регистрации на форумах и социальных сетях, оформления различных подписок и т.д.);

в случае подозрительных ситуаций проверить статистику подключений и изменить пароль.

Не рекомендуется реагировать на письма от неизвестных отправителей, открывать подозрительные вложения к письму (при необходимости вложенные ссылки либо файлы следует проверять на наличие вирусов с помощью специализированных онлайн-сервисов, а также отправлять в открытом виде важные данные (фотоизображения документов, пароли и т. д.).

Безопасность средств парольной защиты:

создавать персональные (уникальные) пароли к разным сервисам;

использовать сложные пароли (например, одновременно будут строчные и заглавные буквы, цифры, специальные знаки (~ ! @ # $ % & *);

регулярно производить смену паролей.

Не рекомендуется: хранить пароли на бумажных носителях, рабочем столе компьютера и в других легкодоступных местах, а также передавать их кому-либо; использовать повторения символов; использовать в качестве пароля свой логин (имя пользователя, учетной записи, никнейм, дату рождения и т.д.); сохранять пароль автоматически в браузере; использовать биографическую информацию и сведения, размещенные в социальной сети.

Безопасность в сети Интернет:

использовать только защищенное соединение HTTPS (проверять, чтобы в адресной строке браузера была зеленая или серая иконка замка);

производить регулярное обновление антивирусного программного обеспечения; обращать внимание при авторизации на доменное имя интернет-ресурса (может произойти подмена имени сайта), в результате чего могут быть скомпрометированы ваши логин, пароль и иные критически важные данные;

отключить общий доступ и использовать надежный пароль для доступа к вашей Wi-Fi точке;

деактивировать автоматическое подключение своих устройств к открытым Wi-Fi точкам;

осуществлять проверку на наличие чужих (не доверенных) устройств в списке подключенных клиентов на роутере.

Не рекомендуется: переходить по непроверенным ссылкам и посещать сайты сомнительного содержания; открывать всплывающие окна, рекламные баннеры и устанавливать предлагаемое неизвестными сайтами программное обеспечение; вводить свой логин и пароль доступа к учетной записи (странице) или системе дистанционного банковского обслуживания при подключении к бесплатным (открытым) точкам Wi-Fi в кафе, транспорте, торговых центрах и т. д.

Использование социальных сетей и интернет-мессенджеров:

целесообразно скрывать персональную и контактную информацию о себе (номер телефона, адрес электронной почты, цифровое фото и другие сведения) в открытом доступе (аккаунт в социальной сети рекомендуется сделать закрытым);

обмениваться сообщениями в социальных сетях и мессенджерах только полностью удостоверившись в личности собеседника, не реагируя на сомнительные просьбы и предложения.

Не рекомендуется: использовать указание геолокации на фото и постах; размещать в сети Интернет объявления с указанием используемых номеров телефонов, а также указывать контактные данные мессенджеров (в случае размещения – удалять сразу же по миновании надобности).

Безопасность мобильных устройств:

использовать пин-код, а также дополнительные способы блокирования устройства (графический ключ, пароль и др.);

своевременно обновлять операционную систему устройства, антивирусное и иное программное обеспечение;

устанавливать приложения только из проверенных источников; обращать внимание, к каким функциям гаджета приложение запрашивает доступ; включить встроенные функции устройства для определения его местонахождения;

в случае утери (хищения) устройства, незамедлительно сменить пароли к интернет-банкингу, электронной почте и другим сервисам;

при смене абонентского номера обязательно изменить привязку интернет-сервисов к новому номеру (лучше сделать это заблаговременно);

при продаже устройства произвести его сброс до заводских настроек.

Не рекомендуется: передавать незнакомым мобильный телефон или сим-карту (в случае передачи – контролировать все действия, которые производятся с устройством); устанавливать приложения с низким рейтингом и отрицательными отзывами; перезванивать на незнакомые иностранные номера; хранить важную информацию на мобильном устройстве; делать полное снятие ограничений на устройстве.

Касаясь **технических мер безопасности** необходимо отметить, что их основная **цель** – обеспечить конфиденциальность, целостность и доступность информации.

Конфиденциальность информации *– это обеспечение доступа к информации только авторизованным пользователям.*

Целостность информации *– это состояние информации, при котором отсутствует любое ее изменение, либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.*

Одним из известных способов проверки целостности информации является использование хэш-функции. Функции, осуществляющей преобразование массива входных данных произвольной длины в выходную установленной длины, выполняемое определенным алгоритмом.

Доступность информации *– это состояние информации (ресурсов автоматизированной информационной системы), при котором субъекты, имеющие права доступа, могут реализовывать их беспрепятственно, но в рамках предоставленных им прав.*

К правам доступа относятся: право на чтение, изменение, копирование, уничтожение информации, а также права на изменение, использование, уничтожение ресурсов. Говоря о методах обеспечения доступности, следует упомянуть системы бесперебойного питания, решения для резервного копирования, резервирования и дублирования мощностей. Кроме того, доступность может быть нарушена злоумышленниками извне, например, путем осуществления DDOS-атак на веб-сайты. Для защиты от таких атак требуется применять специальные программно-аппаратные решения.

Иногда угрозы ИБ возникают из-за халатности сотрудников, которые забывают (теряют) МНИ с информацией, а также из-за техногенных сбоев, например, отключения электричества, или непреднамеренных ошибок при написании программного обеспечения.

Система обеспечения ИБ в первую очередь нацелена на преднамеренные угрозы, исходящими от внешних и внутренних источников. К ним могут относиться применение вредоносного программного обеспечения с целью заражения компьютера (например, вирусами-шифровальщиками); SQL-

инъекция при атаке на веб-сайт; использование снифферов, которые собирают и анализируют трафик из локальной сети; кей-логгеров, фиксирующих ввод данных с клавиатуры и несанкционированные RDP (англ. Remote Desktop Protocol — протокол удаленного рабочего стола).

Технические меры безопасности в области ИБ можно сгруппировать в три основные категории:

технические меры по защите информационных систем и сетей, такие как брандмауэры, антивирусное программное обеспечение, системы обнаружения/предотвращения вторжений и т. д.

технические меры по защите данных, такие как шифрование, контроль доступа, системы резервного копирования и восстановления и т. д.

технические меры для защиты коммуникаций, таких как безопасные протоколы передачи данных, безопасная электронная почта, виртуальные частные сети и т. д.

Реализация этих технических мер требует аудита безопасности для выявления потенциальных угроз и уязвимостей с последующей реализацией мер по устранению или снижению этих рисков. Также важно регулярно отслеживать системы и обновлять меры безопасности по мере необходимости, чтобы не отставать от постоянно меняющегося ландшафта угроз. Кроме того, должна быть разработана комплексная политика безопасности, определяющая допустимое использование информационных систем, обязанности сотрудников по обеспечению безопасности и процедуры реагирования на инциденты.

Для обеспечения эффективности технических мер безопасности также важно регулярно проводить тестирование безопасности, например, оценку уязвимостей, тестирование на проникновение и аудит безопасности. Это помогает выявить слабые места или пробелы в системе безопасности и предпринять корректирующие действия до того, как произойдет нарушение безопасности. Кроме того, важно иметь комплексный план аварийного восстановления, чтобы обеспечить быстрое восстановление информационных систем в случае нарушения безопасности или стихийного бедствия.

Технические меры безопасности играют решающую роль в обеспечении конфиденциальности, целостности и доступности информации. Однако они

должны быть дополнены эффективными организационными, правовыми мерами для создания всеобъемлющей и эффективной основы ИБ.

ГЛАВА 2.

КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ И БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ

2.1. Основные угрозы безопасности информационных систем

Защита информации осуществляется путём принятия правовых, организационных и технических мер, направленных на предотвращение утечки информации, неправомерного воздействия на информацию (уничтожения, модифицирования (искажения, подмены) информации) и неправомерного блокирования доступа к информации.

Целью защиты информации является предотвращение ущерба собственнику, распорядителю, пользователю ИС в результате возможного нарушения целостности (неизменяемости), конфиденциальности и доступности обрабатываемой информации и (или) поддерживающей ее инфраструктуры.

Целостность, конфиденциальность, доступность являются неотъемлемыми компонентами триады ИБ, определяющей состояние защищенности информации. Нарушение либо устранение хотя бы одного элемента в указанной триаде может привести к реализации угрозы безопасности – возможности ее утраты (разрушения, уничтожения), утечки (извлечения, копирования), искажения (модификации, подделки) или блокирования.

Угроза нарушения конфиденциальности реализуется в случае, если информация становится известной лицу, не имеющему полномочий на ознакомление с ней либо получение соответствующего доступа.

Угроза нарушения целостности реализуется при несанкционированном изменении информации, хранящейся либо обрабатываемой в ИС. Целостность информации нарушается как в случае преднамеренного изменения информации злоумышленником, так и в результате случайной ошибки программного или аппаратного обеспечения. Если изменения сделаны уполномоченным лицом с

обоснованной целью (например, плановое обновление ПО, корректировка содержимого базы данных и пр.), то такие изменения являются санкционированными.

Угроза нарушения доступности реализуется, когда в результате преднамеренных действий, предпринимаемых другим пользователем или злоумышленником, блокируется доступ к конкретному информационному ресурсу, службе либо сервису ИС. Блокирование может быть как постоянным (запрашиваемый ресурс никогда не будет получен), так и временным (задержка запрашиваемого ресурса настолько длительная, что он становится бесполезным для авторизованного пользователя).

Основными источниками угроз ИБ ИС являются:

непреднамеренные (ошибочные, случайные, необдуманные, без злого умысла и корыстных целей) нарушения установленных регламентов сбора, обработки и передачи информации, а также требований ИБ и другие действия пользователей (в том числе администраторов средств защиты), приводящие к непроизводительным затратам времени и ресурсов, разглашению сведений ограниченного распространения, потере ценной информации или нарушению работоспособности отдельных рабочих СВТ, подсистем или ИС в целом;

преднамеренные (в корыстных целях, по принуждению третьими лицами, со злым умыслом и т. п.) действия пользователей, допущенных к работе с ведомственными ИС, а также работников, отвечающих за обслуживание, администрирование программного и аппаратного обеспечения, средств защиты и обеспечения ИБ;

ошибки, допущенные при проектировании ИС и её системы защиты, ошибки в ПО, отказы и сбои технических средств (в том числе средств защиты информации и контроля эффективности защиты) ИС;

аварии, стихийные бедствия и т.п.

Основные пути реализации непреднамеренных искусственных (субъективных) угроз ИС:

действия пользователей, приводящие к частичному или полному отказу системы или нарушению работоспособности аппаратных или программных средств; отключению оборудования или изменение режимов работы устройств

и ПО; разрушению информационных ресурсов ИС (неумышленная порча оборудования, удаление, искажение программ или файлов с важной информацией, в том числе системных, повреждение каналов связи, неумышленная порча МНИ и т.п.);

несанкционированный запуск технологического ПО, способного при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или осуществляющих необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.);

несанкционированное внедрение и использование неучтенного ПО (игровые, обучающие, технологические и другие, не являющиеся необходимыми для выполнения пользователями ИС своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (процессорного времени, оперативной памяти, памяти на внешних носителях и т.п.);

разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования или ЭЦП, идентификационных карточек, пропусков и т.п.);

игнорирование организационных ограничений (установленных правил) при работе с ИС;

некомпетентное использование, настройка или неправомерное отключение средств защиты ответственными за ИБ;

ввод ошибочных данных.

Преднамеренные информационные угрозы могут быть реализованы злоумышленником в ходе осуществления следующих мероприятий:

использование программно-технических средств, выполняющих обращение к объектам доступа в обход средств защиты ИС;

модификация средств защиты ИС, позволяющая реализовать угрозы ИБ;

внедрение программных или технических средств (алгоритмов), нарушающих исходную структуру и функции ИС (в том числе и средств защиты).

Методы реализации преднамеренных угроз ИБ ИС могут основываться на

следующих основных подходах:

первоначальная разведка среды (получение злоумышленником детальной информации о функциях, выполняемых ИС, о применяемых системах защиты, о программно-аппаратной среде, типе и параметрах ИС, типе и версии ОС, составе прикладного ПО и т. п.);

мониторинг ИС и визуальное наблюдение за объектами доступа;

хищение (копирование) МНИ, содержащих информацию, представляющую интерес;

использование специальных технических средств для перехвата ПЭМИН – нежелательных радиоизлучений, возникающих в результате нелинейных процессов в компонентах ТСОИ (средства вычислительной и организационной техники);

перехват данных, передаваемых по каналам связи;

НСД к ресурсам ИС в обход или путем преодоления систем защиты с использованием специальных средств, приемов, методов;

внесение пользователем несанкционированных изменений в программно-аппаратные компоненты ИС и обрабатываемые данные;

установка и использование нештатного аппаратного и/или ПО;

заражение ВПО;

выведение из строя МНИ без уничтожения и др.

Модель возможного нарушителя ИБ.

Гарантией построения адекватной системы обеспечения ИБ ИС является правильно разработанная модель нарушителя. Нарушитель – это лицо, которое предприняло попытку выполнения запрещенных операций (действий) по ошибке, незнанию или осознанно со злым умыслом (из корыстных интересов) или без такового (ради игры или удовольствия, с целью самоутверждения и т. п.) и использующее для этого различные возможности, методы и средства.

Модель нарушителя ИБ *– это набор предположений об одном или нескольких возможных нарушителях ИБ, их квалификации, используемых ими технических и материальных средствах и т. д.*

Система защиты ИС должна строиться исходя из предположений о следующих возможных типах нарушителей в системе (с учетом категории лиц, мотивации, квалификации, наличия специальных средств и др.):

Неопытный (невнимательный) пользователь – зарегистрированный пользователь ИС, который может предпринимать попытки выполнения запрещенных операций, доступа к защищаемым ресурсам ИС с превышением своих полномочий, ввода некорректных данных и т. п. действия по ошибке, некомпетентности или халатности без злого умысла и использующий при этом только штатные (доступные ему) аппаратные и программные средства.

Любитель – зарегистрированный пользователь ИС, пытающийся преодолеть систему защиты без корыстных целей и злого умысла, для самоутверждения или «из интереса». Для преодоления системы защиты и совершения запрещенных действий может использовать различные методы получения дополнительных полномочий доступа к ресурсам (имен, паролей и т. п. других пользователей), недостатки в построении системы защиты и доступные ему штатные (установленные на рабочей СВТ) программы (несанкционированные действия посредством превышения своих полномочий на использование разрешенных средств). Помимо этого, может пытаться использовать дополнительно нештатные инструментальные и технологические программные средства (отладчики, служебные утилиты), самостоятельно разработанные программы или стандартные дополнительные технические средства.

«Мошенник» – зарегистрированный пользователь ИС, который может предпринимать попытки выполнения незаконных технологических операций, ввода подложных данных и тому подобные действия в корыстных целях, по принуждению или из злого умысла, но использующий при этом только штатные (установленные на рабочей станции и доступные ему) аппаратные и программные средства от своего имени или от имени другого работника (зная его имя и пароль, используя его кратковременное отсутствие на рабочем месте и т.п.).

Внутренний злоумышленник – зарегистрированный пользователь ИС, действующий целенаправленно из корыстных интересов или мести за

нанесенную обиду, возможно, в сговоре с лицами, не являющимися сотрудниками ОВД либо пользователями ИС. Может использовать весь набор методов и средств взлома системы защиты, включая несанкционированные методы получения реквизитов доступа, пассивные средства (технические средства перехвата без модификации компонентов системы), методы и средства активного воздействия (модификация технических средств, подключение к каналам передачи данных, внедрение программных закладок и использование специальных инструментальных и технологических программ), а также комбинации воздействий как изнутри, так и извне – из сетей общего пользования.

Внутренним нарушителем может быть лицо из следующих категорий пользователей ИС:

зарегистрированные пользователи ИС;

сотрудники, не допущенные к работе с ИС;

персонал, обслуживающий технические средства ИС (инженеры, техники);

работники подразделений разработки и сопровождения ПО (прикладные и системные программисты);

технический персонал, обслуживающий здания (уборщицы, электрики, сантехники и другие работники, имеющие доступ в здания и помещения, где расположены компоненты ИС);

сотрудники и подразделения ИБ;

руководители различных уровней.

Внешний нарушитель (злоумышленник) – постороннее лицо или зарегистрированный пользователь ИС, действующий целенаправленно из корыстных интересов, из мести или из любопытства, возможно в сговоре с другими лицами. Он может использовать весь набор способов нарушения ИБ, методов и средств взлома систем защиты, характерных для сетей общего пользования (в особенности сетей на основе IP-протокола), включая удаленное внедрение программных закладок и использование специальных инструментальных и технологических программ, используя имеющиеся слабости протоколов обмена и системы защиты узлов сети АИ.

Категории лиц, которые могут быть внешними нарушителями:

уволенные сотрудники ОВД;

представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности подразделения ОВД (энерго-, водо-, теплоснабжения и т. п.);

посетители (приглашенные граждане, представители организаций, поставляющих технику, ПО, услуги и т. п.);

криминальные структуры; зарубежные спецслужбы или лица, действующие по их заданию;

лица, случайно или умышленно проникшие в сети ИС из внешних (по отношению к ЕЦП) сетей телекоммуникации («хакеры»).

Пользователи и обслуживающий персонал из числа сотрудников ОВД либо гражданского персонала имеют наиболее широкие возможности по осуществлению несанкционированных действий, вследствие наличия у них определенных полномочий по доступу к ресурсам и хорошего знания технологии обработки информации и защитных мер. Действия этой группы лиц напрямую связано с нарушением действующих правил и инструкций. Особую опасность эта группа нарушителей представляет при взаимодействии с криминальными структурами или зарубежными спецслужбами.

Уволенные сотрудники (работники) могут использовать для достижения целей свои знания о технологии работы, защитных мерах и правах доступа. Полученные в подразделениях ОВД знания и опыт выделяют их среди других источников внешних угроз.

Криминальные структуры представляют наиболее агрессивный источник внешних угроз. Для осуществления своих замыслов эти структуры могут идти на открытое нарушение закона и вовлекать в свою деятельность сотрудников ОВД либо гражданский персонал всеми доступными им силами и средствами.

Профессиональные «хакеры» имеют высокую техническую квалификацию и знания об уязвимостях программных средств, используемых в ИС. Наибольшую угрозу представляют при взаимодействии с работающими и уволенными работниками подразделения ОВД и криминальными структурами.

Организации, занимающиеся разработкой, поставкой и ремонтом оборудования, ИС, представляют внешнюю угрозу в силу того, что эпизодически имеют непосредственный доступ к информационным ресурсам. Криминальные структуры и спецслужбы могут использовать эти организации для временного устройства на работу своих членов, с целью доступа к защищаемой информации в ИС.

Кроме этого, оцениваются реальные технические возможности злоумышленника для воздействия на систему защиты или на защищаемый объект. Под техническими возможностями подразумевается перечень различных технических средств, которыми может располагать нарушитель в процессе совершения действий, направленных против системы информационной защиты.

Принимаются следующие ограничения и предположения о характере действий возможных нарушителей:

работа по подбору персонала и специальные проверочные мероприятия исключают возможность создания сообществ нарушителей, т.е. объединения (сговора) и целенаправленных действий двух и более нарушителей;

нарушитель скрывает свои несанкционированные действия от других сотрудников;

несанкционированные действия могут быть следствием ошибок пользователей, администраторов безопасности, эксплуатирующего и обслуживающего персонала, а также недостатков принятой технологии обработки, хранения и передачи информации;

в своей противоправной деятельности вероятный нарушитель может использовать любое имеющееся средство перехвата информации, воздействия на информацию и ИС, адекватные финансовые средства для подкупа персонала, шантаж и другие средства и методы для достижения стоящих перед ним целей.

2.2. Каналы утечки информации: виды, содержание, особенности реализации

Степень защиты информации, обрабатываемой в ИС, определяется полнотой перекрытия всего спектра КУИ, предопределяющих возможные пути обхода средств защиты с целью нарушения свойств, обеспечивающих безопасность информации. Необходимым условием реализации комплексного подхода к обеспечению ИБ является блокирование найденных (выявленных) КУИ, поэтому для создания эффективных систем безопасности, в первую очередь, необходимо исследовать возможные каналы утечки информации, осуществить анализ их характеристик.

Учитывая природу источника данных и соответствующих информативных сигналов, различают следующие ***каналы утечки информации:***

физические,

технические,

информационные.

Физический КУИ возникает из-за недостаточной защиты бумажных либо МНИ в процессе их хранения или использования в повседневной деятельности. Реализация этого КУИ позволяет злоумышленникам осуществлять НСД к информации. Источниками информации могут быть выносимые за пределы рабочей зоны материальные объекты: бумажные документы, фотографии, МНИ и т. п.

Технический КУИ представляет собой совокупность источника информации, материального носителя или среды распространения несущего указанную информацию сигнала и средства выделения информации из сигнала или носителя. Источниками информации для такого канала могут быть различные шумовые сигналы, излучения и вибрации, исходящие от интересующих объектов. Физические процессы, происходящие в технических средствах при их функционировании, создают в окружающем пространстве излучения, которые в той или иной степени связаны с обрабатываемой информацией (акустическое и электромагнитное излучение, ПЭМИН и др.). С

учетом того, что неконтролируемое распространение информативного сигнала от его источника происходит через определенную физическую среду (волновую или электрическую), для выявления и последующей расшифровки информационных сигналов используется специальная техника.

Информационные КУИ появляются из-за несоблюдения правил обработки, хранения и передачи информации, а также в результате использования недостаточно защищенного ПО. Результатом реализации такого КУИ может стать НСД к ресурсам ИС, что позволит злоумышленнику осуществить копирование, искажение, блокирование либо уничтожение информации и (или) поддерживающей ее инфраструктуры.

Одной из ключевых угроз безопасности информации ограниченного распространения, обрабатываемой в ИС, является утечка информации по ТКУИ. Повышенная опасность их функционирования обусловлена широкой вариативностью (разнообразием) источников возникновения информационных сигналов, характеристиками среды их распространения и способами их обнаружения.

Рассмотрим обобщённую типовую структуру функционирования ТКУИ (рис. 1).

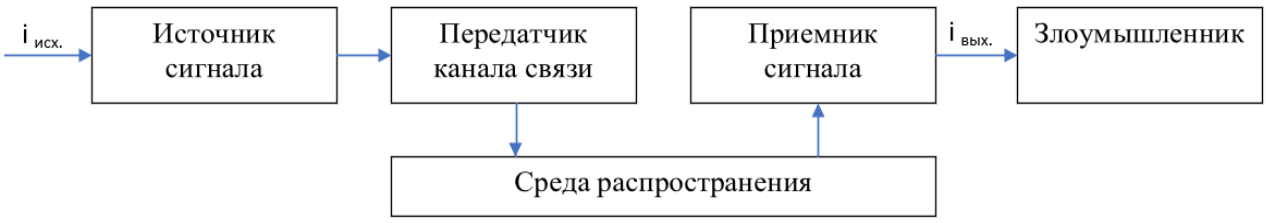


Рис. 1. Типовая структура ТКУИ, обрабатываемой в ИС

На вход ТКУИ поступает информация с ограниченного распространения в виде исходного сигнала $i_{исх}$. Исходный сигнал может поступать как с некоторого информационного носителя, так и с выхода предыдущего канала.

Источником сигнала $i_{исх}$ могут выступать:

объект наблюдения, отражающий акустические, виброакустические, электромагнитные волны;

объект наблюдения, излучающий собственные электромагнитные волны в оптическом и радиодиапазонах;

После того, как информация от источника поступает на вход КУИ (в виде буквенно-цифрового текста, символов, знаков, звуков, сигналов и т. д.), передатчик функционального канала связи осуществляет преобразование полученной информации в форму, обеспечивающую запись ее на носитель информации, соответствующий среде распространения.

В общем случае он выполняет следующие функции:

создает (генерирует) поля (акустическое, электромагнитное) или электрический ток, которые переносят информацию;

осуществляет запись информации на МНИ;

усиливает мощность сигнала (носителя с информацией);

обеспечивает передачу (излучение) сигнала в среду распространения в заданном секторе пространства.

Приемник сигнала выполняет функции, обратные функциям передатчика. Он производит следующие действия:

осуществляет выбор носителя с нужной получателю информацией;

усиливает принятый сигнал до значений, обеспечивающих качественный съем информации;

выполняет съем информации с носителя;

преобразование информации в форму сигнала, доступную получателю (человеку, техническому устройству), и усиление сигналов до значений, необходимых для безошибочного их восприятия.

Следовательно, в любых ТСОИ существуют те или иные ТКУИ, которые в соответствии со своей физической природой способны порождать и дополнительные каналы утечки. Знание различных видов ТКУИ и их особенностей позволяет решать задачу определения возможных неконтролируемых проявлений физических полей, образующих КУИ.

Особенности ТКУИ определяются физической природой возникновения информационных сигналов, характеристиками среды их распространения и способами их выявления. Общая классификация ТКУИ включает следующие виды каналов (рис. 2):

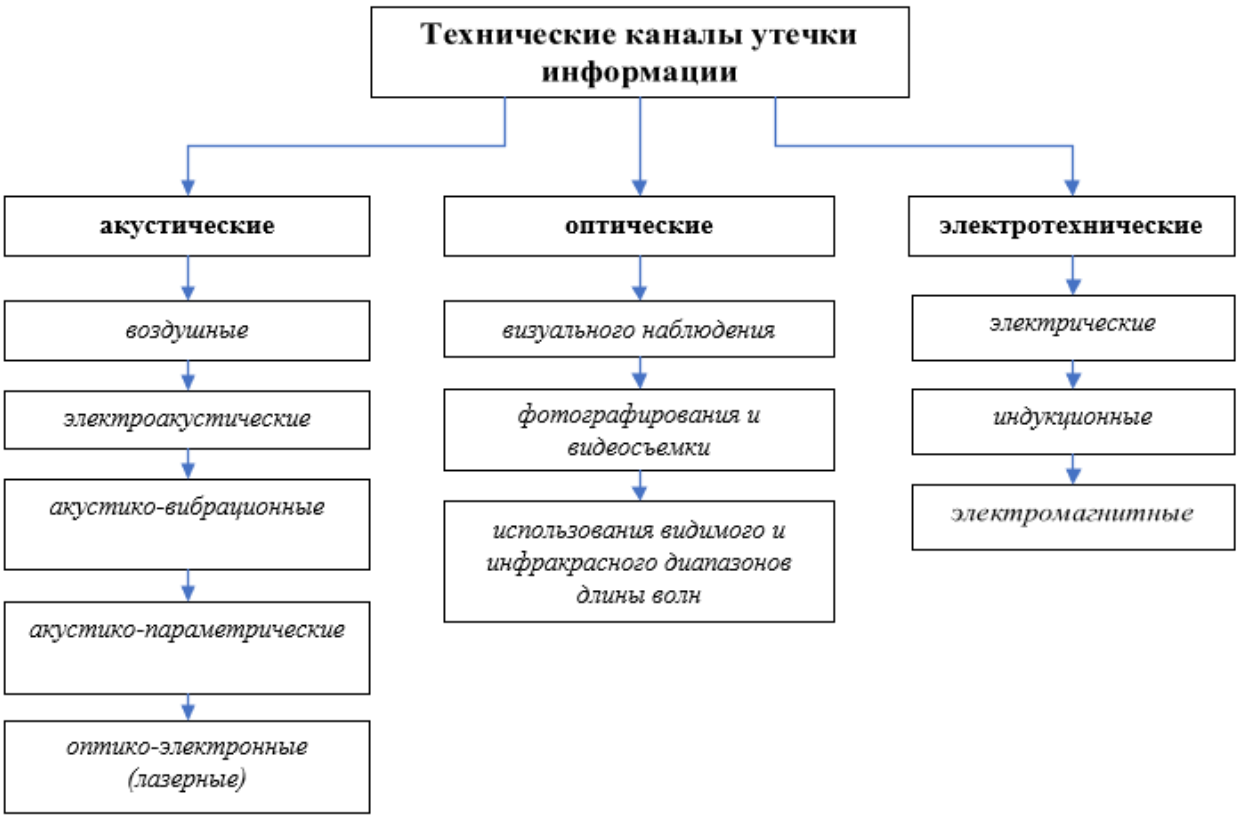


Рис. 2. Общая классификация ТКУИ, обрабатываемой в ИС

акустические (образуются при распространении звуковых волн в воздухе или упругих колебаний в других средах; детерминируют соответствующие основным характеристикам звука механические колебания стен, перекрытий, трубопроводов, окон и т. д.);

оптические (основаны на перехвате информации видимого и инфракрасного диапазонов длин волн с помощью оптических приборов);

электротехнические (средой переноса информативных сигналов могут быть электрический ток или электромагнитные поля с частотами в радиодиапазоне, побочные электромагнитные излучения, индуктивные наводки).

Рассмотрим указанные ТКУИ более подробно.

Акустические ТКУИ. Носителем информации является акустический сигнал – возмущение упругой среды, проявляющееся в возникновении акустических колебаний различной формы и длительности. В случае, когда источником информации является голосовой аппарат человека, информация

называется речевой. Речевой сигнал является сложным акустическим сигналом, основная энергия которого сосредоточена в диапазоне частот от 300 Гц до 4000 Гц. Под действием акустических колебаний в ограждающих строительных конструкциях и инженерных коммуникациях помещения, в котором находится речевой источник, возникают вибрационные колебания. Таким образом, в своем первоначальном состоянии речевой сигнал в помещении присутствует в виде акустических и вибрационных колебаний.

Различают следующие виды технических каналов утечки акустической информации:

воздушные (средой распространения акустических сигналов является воздух, и для их перехвата используются миниатюрные высокочувствительные направленные микрофоны, которые соединяются с портативными звукозаписывающими устройствами или специальными миниатюрными передатчиками (рис. 3). Автономные устройства, конструктивно объединяющие микрофоны и передатчики, называют закладными устройствами перехвата речевой информации. Перехваченная речевая информация может передаваться по радиоканалу, сети электропитания, соединительным линиям ВТСС и др.);

электроакустические (возникают за счет электроакустических преобразований акустических сигналов в электрические и включают перехват акустических колебаний через ВТСС. Обусловлен тем, что некоторые элементы ВТСС (например, трансформаторы, катушки индуктивности, звонки аналоговых телефонных аппаратов и т. п.) обладают свойством изменять свои параметры (емкость, индуктивность, сопротивление) под действием акустического поля, создаваемого источником речевого сигнала. Изменение параметров приводит либо к появлению на данных элементах электродвижущей силы, либо к модуляции токов, протекающих по этим элементам, в соответствии с изменениями воздействующего акустического поля.

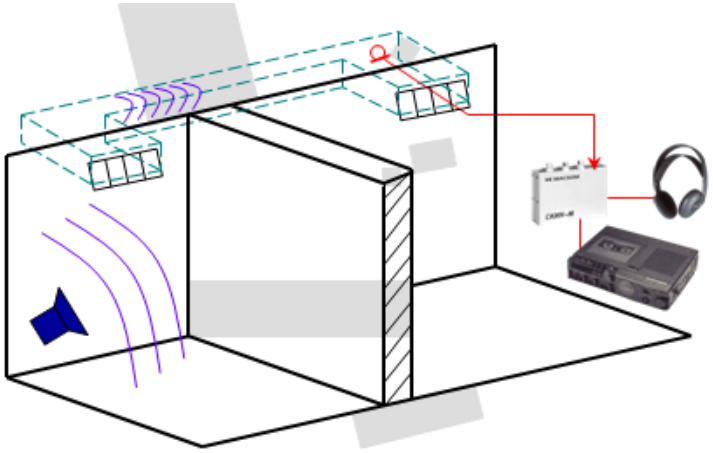


Рис. 3. Схема функционирования воздушного канала утечки акустической информации.

Перехват акустоэлектрических колебаний в данном канале утечки информации осуществляется путем непосредственного подключения к соединительным линиям ВТСС специальных высокочувствительных низкочастотных усилителей. Например, подключая такие средства к соединительным линиям телефонных аппаратов с электромеханическими вызывными звонками, можно прослушивать разговоры, ведущиеся в помещениях, где установлены эти аппараты (рис. 3);

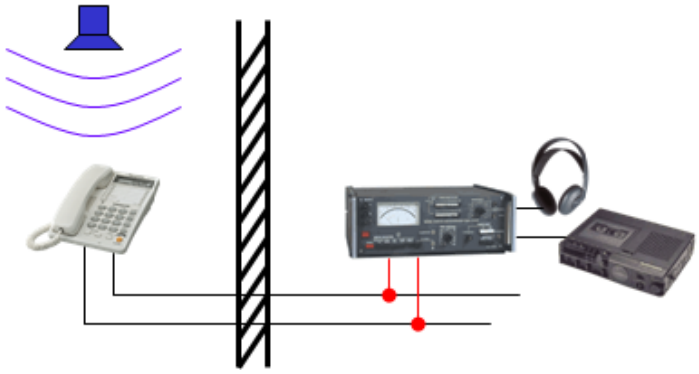


Рис. 3. Схема функционирования электроакустического канала утечки акустической информации.

акустико-вибрационные (средой распространения акустических сигналов являются конструкции зданий, сооружений (стены, потолки, полы), трубы

водоснабжения, отопления, канализации и другие твердые тела. Для перехвата акустических колебаний в этом случае используются контактные микрофоны (стетоскопы) (рис. 4));

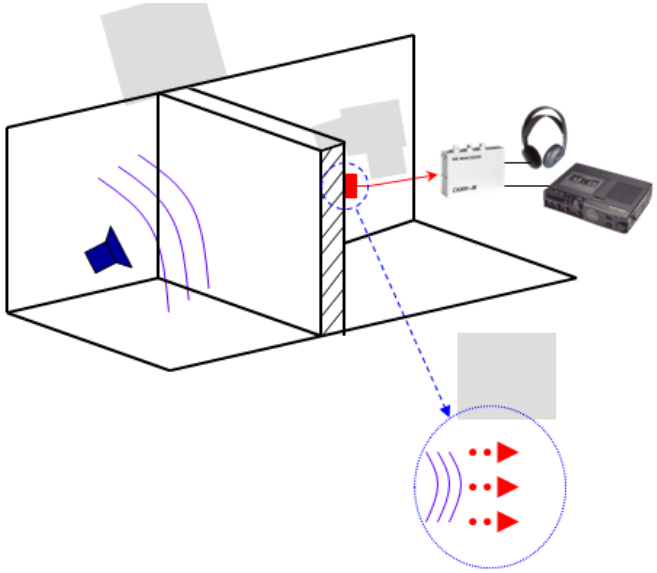


Рис. 4. Схема функционирования акустико-вибрационного канала утечки акустической информации.

акустико-параметрические (образуются в результате воздействия акустического поля на элементы высокочастотных генераторов и изменения взаимного расположения элементов схем, проводов, дросселей и т. п., что приводит к изменениям параметров сигнала, например, модуляции его информационным сигналом. Соответствующие высокочастотные колебания излучаются в окружающее пространство и могут быть перехвачены, а затем выделены специальными средствами) (рис. 5);

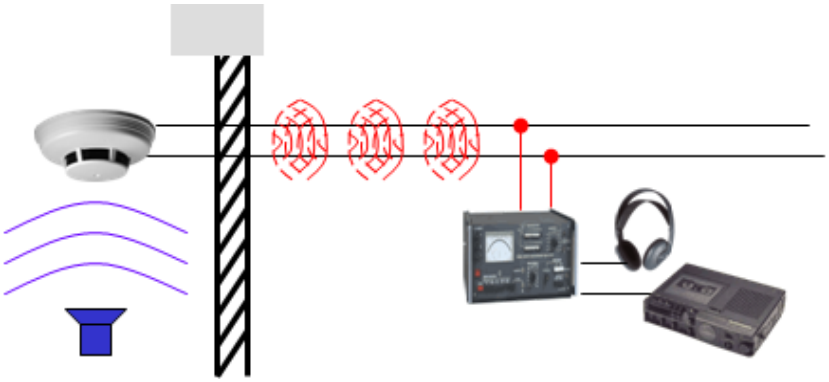


Рис. 5. Схема функционирования акустико-параметрического канала утечки акустической информации.

оптико-электронные (лазерные) (образуются при облучении лазерным лучом вибрирующих в акустическом поле тонких отражающих поверхностей (стекол окон, картин, зеркал и т.д.). Отраженное лазерное излучение (диффузное или зеркальное) модулируется по амплитуде и фазе (по закону вибрации поверхности) и принимается приемником оптического (лазерного) излучения, при демодуляции которого выделяется полезная речевая информация. При этом, лазер и приемник оптического излучения могут быть установлены как в одном, так и разных местах (помещениях) (рис. 6).

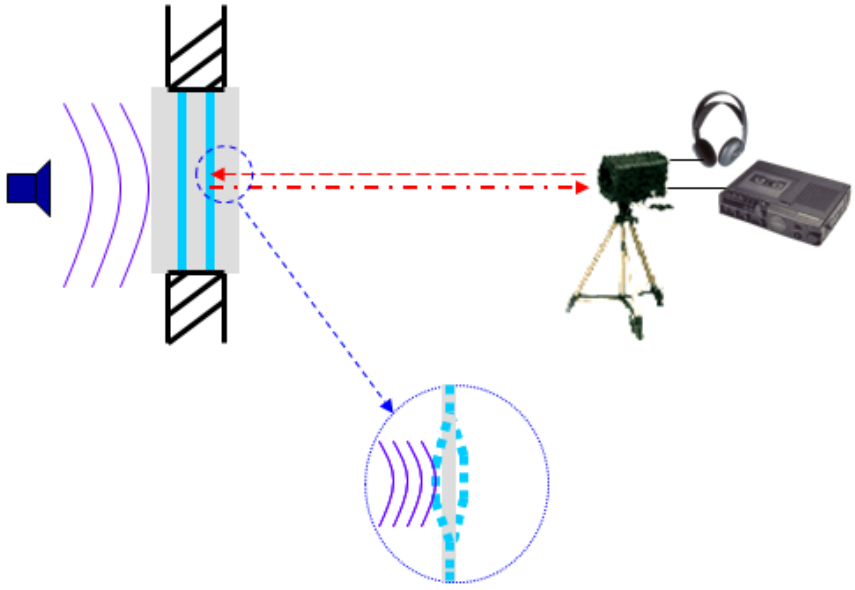


Рис. 6. Схема функционирования оптико-электронного (лазерного) канала утечки акустической информации.

Акустические ТКУИ могут быть источником утечки не только речевой информации. В литературе описаны случаи, когда с помощью статистической обработки акустической информации с клавиатуры удавалось перехватывать компьютерную текстовую информацию, в том числе осуществлять съем информации по системе централизованной вентиляции.

Оптические ТКУИ. В качестве среды распространения в оптическом канале утечки информации обычно выступают: воздух (атмосфера); стекло; оптические световоды.

По способу перехвата информации оптические ТКУИ подразделяют на оптические каналы:

визуального наблюдения (невооруженным глазом или через бинокль);

фотографирования и видеосъемки;

использования видимого и инфракрасного диапазонов длины волн (для передачи информации от скрыто установленных микрофонов и иных датчиков, преобразователей).

Злоумышленники уделяют большое внимание утечке визуальной информации, получаемой в виде изображений объектов или копий документов путем наблюдения за объектом, съемки объекта и съемки (копирования) документов. В зависимости от условий наблюдения ими используются соответствующие технические средства, в том числе: оптика (бинокли, подзорные трубы, телескопы, монокуляры), видеокамеры, приборы ночного видения, тепловизоры и т. п. Для документирования результатов наблюдения проводится съемка объектов с помощью фотографических и телевизионных средств, соответствующих условиям съемки. Для снятия копий документов используются специальные (закамуфлированные) фотоаппараты. Для дистанционного съема видовой информации используют специальные (закамуфлированные) видеокамеры для дистанционного съема видеоинформации – видеозакладки.

Электротехнические ТКУИ. В зависимости от вида функционального канала связи электротехнические ТКУИ можно разделить на электромагнитные, электрические и индукционные.

Электрические каналы утечки предполагают перехват информации путём непосредственного подключения специальных электронных устройств к соединительным линиям вспомогательных технических средств и систем, а также посторонним проводникам.

Электронные устройства перехвата информации по электрическим

каналам утечки информации обычно именуются аппаратными закладками. Они представляют собой миниатюрные передатчики, излучение которых модулируется информационным сигналом. Перехваченная с помощью закладных устройств информация непосредственно передаётся по радиоканалу или сначала записывается на специальное запоминающее устройство, а уже затем по команде передаётся на запросивший её объект.

Электрический канал утечки информации, передаваемой по кабельным линиям связи, предполагает контактное подключение к этим линиям. В этом случае такой канал обычно используется для перехвата телефонных разговоров, при этом перехватываемая информация может быть записана на диктофон или передана по радиоканалу. Подобные устройства, подключаемые к телефонным линиям связи и содержащие радиопередатчики для ретрансляции перехваченной информации, обычно называются *телефонными закладками*.

Очевидно, что контактное электрическое подключение технических средств съема информации в ряде случаев может являться компрометирующим признаком. В этой связи злоумышленники используют *индукционный канал* утечки информации, который не требует непосредственного подключения к каналам связи. Индукционный канал эксплуатирует эффект возникновения вокруг высокочастотного кабеля электромагнитного поля при прохождении информационных сигналов. Для перехвата информации используются специальные индукционные датчики (рис.7), устанавливаемые вблизи соответствующих линий связи. Данный канал широко используется для прослушивания телефонных разговоров, ведущихся по проводным и радио/радиорелейным линиям связи.

Рис. 7. Индуктивный датчик в цилиндрическом корпусе с повышенной чувствительностью

(с кабелем 0,3 м и разъемом М12)

В *электромагнитных каналах* утечки информации носителем информации являются электромагнитные излучения, возникающие при обработке информации техническими средствами. Каждое электрическое (электронное) устройство является источником магнитных и электромагнитных полей широкого спектра, характер которых определяется назначением и схемными решениями, мощностью устройства, материалами, из которых оно изготовлено, и его конструкцией.

Технические средства перехвата информации могут быть внедрены злоумышленником следующими способами:

установка средств перехвата информации в ограждающие конструкции помещений во время строительных, ремонтных и профилактических работ. При этом в качестве исполнителей могут быть использованы сотрудники соответствующих служб и организаций;

установка средств перехвата информации в предметы мебели, интерьера и обихода (в том числе, которые вручаются в качестве подарков, а впоследствии могут использоваться для оформления интерьера служебных помещений), а также различные технические средства общего назначения (телефон, компьютер, телевизор и т. д.).

Наиболее опасными с точки зрения защищенности ИС могут быть следующие виды излучений и наводок:

электромагнитные излучения элементов ТСОИ (носителем информации является электрический ток, напряжение, частота или фаза которого изменяются по закону информационного сигнала);

электромагнитные излучения на частотах работы высокочастотных генераторов ТСОИ и ВТСС (в результате внешних воздействий информационного сигнала на элементах генераторов наводятся электрические сигналы, которые могут вызвать непреднамеренную модуляцию собственных высокочастотных колебаний генераторов и излучение в окружающее пространство);

электромагнитные излучения на частотах самовозбуждения усилителей

низкой частоты ТСПИ (самовозбуждение возможно за счет случайных преобразований отрицательных обратных связей в паразитные положительные, что приводит к переводу усилителя из режима усиления в режим автоматической генерации сигналов);

наводки электромагнитных излучений ТСОИ (возникают при излучении элементами ТСОИ информационных сигналов, а также при наличии гальванической связи соединительных линий ТСОИ и посторонних проводников или линий ВТСС);

просачивание информационных сигналов в цепи электропитания (возможно при наличии магнитной связи между выходным трансформатором усилителя и трансформатором электропитания, а также за счет неравномерной нагрузки на выпрямитель, что приводит к изменению потребляемого тока по закону изменения информационного сигнала);

просачивание информационных сигналов в цепи заземления (образуется за счет гальванической связи с землей различных проводников, выходящих за пределы КЗ, в том числе нулевого провода сети электропитания, экранов, металлических труб систем отопления и водоснабжения, металлической арматуры и т. п.);

съем информации с использованием закладных устройств, представляющих собой миниатюрные радиопередатчики, устанавливаемые в ТСОИ, излучения которых модулируются информационным сигналом и принимаются за пределами КЗ.

Основными причинами возникновения электромагнитных каналов утечки информации в ИС являются:

ПЭМИН, возникающие вследствие функционирования СВТ (вывод информации на экран монитора; ввод данных с клавиатуры; запись информации на накопители; чтение информации с накопителей; передача данных в каналы связи; вывод данных на периферийные устройства – звуковые, печатающие и т. п.;

модуляция информативным сигналом ПЭМИН высокочастотных генераторов ТСОИ;

модуляция информативным сигналом паразитного электромагнитного

излучения ТСОИ (например, возникающего вследствие самовозбуждения усилителей низкой частоты) и др.

Особое внимание следует обратить на перехват информации при ее передаче по каналам связи. Это вызвано тем, что в данном случае обеспечивается свободный НСД к передаваемым сигналам, особенно в случае использования радиоканала. В зависимости от вида канала связи технические каналы перехвата информации можно разделить на электромагнитные, электрические и индукционные.

Электромагнитные излучения передатчиков средств связи, модулированные информационным сигналом, могут перехватываться естественным образом с использованием стандартных технических средств. Электромагнитный канал перехвата информации широко применяется для прослушивания телефонных разговоров, ведущихся по радиотелефонам, сотовым телефонам или по радиорелейным и спутниковым линиям связи.

При оценке степени опасности ТКУИ следует иметь в виду, что не всегда наличие носителя (акустического или электромагнитного поля) является фактором, достаточным для съема информации. Например, при низкой разборчивости речи невозможно восстановить ее смысл. ПЭМИН функционирующих электронных устройств могут не нести информативного сигнала (например, излучение, возникшее вследствие генерации тактовых импульсов СВТ). Для объективной оценки проводят специальные исследования оборудования и специальные проверки рабочих помещений. Такого рода исследования и проверки выполняются организациями, имеющими лицензии на соответствующий вид деятельности. При выявлении ТКУИ применяются меры по их перекрытию.

Информационные КУИ могут быть разделены на следующие виды:

каналы линий связи (коммутируемых, выделенных) и ЛВС;

канал МНИ;

канал терминальных и периферийных устройств ИС.

Указанные КУИ позволяют злоумышленнику реализовать перехват либо НСД к информации, обрабатываемой в ИС. Для этих целей им могут быть использованы следующие программно-аппаратные средства:

аппаратные закладки (электронные устройства перехвата информации, устанавливаемые в ТСОИ);

ВПО (программы, предназначеные для несанкционированного копирования, модификации, блокирования, уничтожения компьютерной информации).

Типичным примером аппаратных закладок являются так называемые аппаратные кейлоггеры – устройства, которые регистрируют нажатия клавиш на клавиатуре компьютера. Они скрытно устанавливаются в самой клавиатуре либо в системном блоке, могут быть также установлены в переходном разъеме, подключаемом в разрыв кабеля, соединяющего клавиатуру и системный блок (рис. 8).

Рис. 8. Аппаратный кейлоггер, встроенный в переходник USB

Перехваченная кейлоггером информация может записываться в память (файл) СВТ, пересылаться по сети либо по радиоканалу передаваться на приемный пункт злоумышленника по команде управления.

Существуют также *программные закладки*, выполняющие одно из перечисленных действий:

копирование информации пользователя ИС (паролей, криптографических ключей, кодов доступа и т. п.);

изменение алгоритмов работы системного, прикладного и служебного ПО (например, изменение программы разграничения доступа может привести к тому, что доступ будет разрешен любому пользователю независимо от правильности пароля);

навязывание определенных режимов работы (например, блокирование записи на жесткий диск при удалении информации, при этом запись не уничтожается и может быть прочитана).

По методу внедрения в СВТ программные закладки подразделяются на:

программно-аппаратные закладки, связанные с аппаратными средствами компьютера (их средой обитания обычно является BIOS);

загрузочные закладки, связанные с программами начальной загрузки, которые располагаются в загрузочных секторах, из которых СВТ при начальной загрузке считывает программу, берущую на себя последующую загрузку самой ОС;

драйверные закладки, внедренные в драйвера аппаратного обеспечения;

прикладные закладки, ассоциированные с прикладным ПО общего назначения (текстовые редакторы, утилиты, программные оболочки и антивирусное ПО);

исполняемые закладки, ассоциированные с исполняемыми программными модулями, содержащими код этой закладки (чаще всего эти модули представляют собой пакетные файлы, которые состоят из команд ОС, выполняемых одна за одной, как если бы их набирали на клавиатуре компьютера);

закладки-имитаторы, интерфейс которых идентичен с интерфейсом некоторых служебных программ, требующих ввод конфиденциальной информации (паролей, криптографических ключей, номеров кредитных карточек);

замаскированные закладки, которые маскируются под программные средства оптимизации работы СВТ (файловые архиваторы, дисковые дефрагментаторы).

При этом можно выделить *резидентные закладки*, которые находятся в оперативной памяти постоянно, начиная с некоторого момента и до окончания работы компьютера, и *нерезидентные закладки*, которые попадают в оперативную память СВТ аналогично резидентным, но выгружаются при выполнении особых условий.

Основные возможности НСД связаны с использованием информациии о потенциальных недостатках (уязвимостях) цели, позволяющей злоумышленнику выбрать подходящий сценарий вредоносной атаки, затем осуществить ее, после чего на заключительном этапе очистить журналы аудита либо заполнить их ложными записями.

Атакой на компьютерную систему будем называть преднамеренные действия, использующие уязвимости в системном, прикладном и сетевом ПО (в том числе уязвимости протоколов сетевого взаимодействия) приводящие к установлению контроля на ОС или осуществления НСД к информации. Атаки на компьютерные системы столь же разнообразны, сколь разнообразны объекты, против которых они направлены. Технологически большинство компьютерных атак использует ряд уязвимостей, изначально присущих системному, прикладному сетевому ПО.

Существуют различные типы классификации атак: пассивные и активные, внешние и внутренние атаки, умышленные и неумышленные. Рассмотрим основные из них (рис. 1).

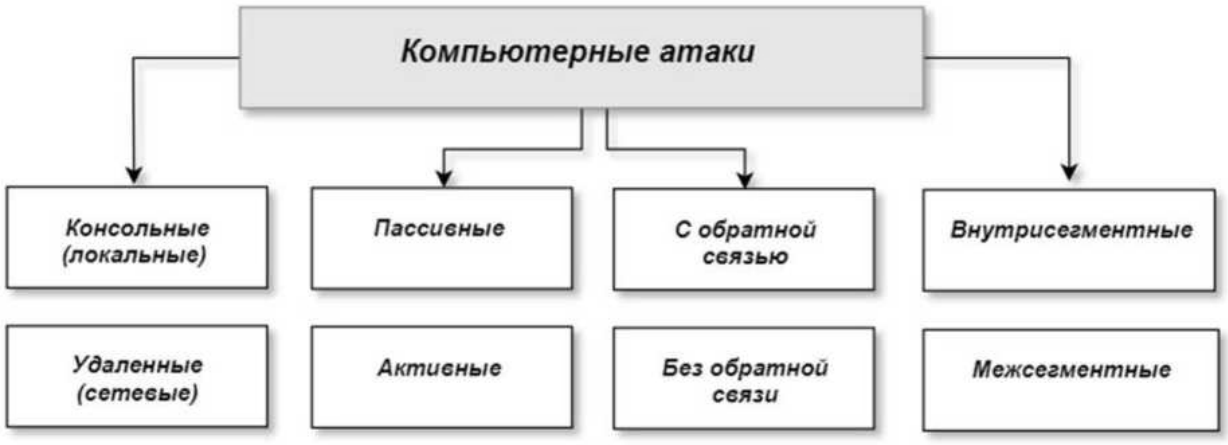


Рис. 1. Классификация компьютерных атак

По расположению атакующего и атакуемой системы:

консольные (локальные) – атаки осуществляются на СВТ, к которому атакующий имеет непосредственный физический доступ;

сетевые (удаленные) – атаки осуществляются через глобальную или локальную сеть, как на СВТ, так и на передаваемую по сети информацию.

По характеру воздействия: пассивные; активные.

Пассивное воздействие представляет собой воздействие, не оказывающее прямого влияния на работу системы, но в то же время способное нарушить ее политику безопасности. Отсутствие прямого влияния на работу приводит именно к тому, что пассивное удаленное воздействие трудно обнаружить. Возможным примером типового пассивного воздействия служит прослушивание канала связи в сети.

Активное воздействие оказывает прямое влияние на работу самой системы (нарушение работоспособности, изменение конфигурации и т. д.), которое нарушает политику безопасности, принятую в ней. Активными воздействиями являются почти все типы удаленных атак. Активное воздействия обнаружить, так как в результате его осуществления в системе происходят некоторые изменения.

По цели воздействия: нарушение функционирования системы (доступа к системе); нарушение целостности информационных ресурсов; нарушение конфиденциальности информационных ресурсов. Этот признак, по сути, является прямой проекцией трех базовых разновидностей угроз – отказа в обслуживании, раскрытия и нарушения целостности.

Существуют два принципиальных варианта получения информации: искажение и перехват. В отличие от искажения, вариант перехвата информации означает получение к ней доступа без возможности ее изменения. Следовательно, перехват информации приводит к нарушению ее конфиденциальности (например, прослушивание канала в сети).

По наличию обратной связи с атакуемым объектом:

с обратной связью – атакующий отправляет некоторые запросы на атакуемый объект, на которые ожидает получить ответ. Следовательно, между атакующим и атакуемым появляется обратная связь, позволяющая первому адекватно реагировать на всяческие изменения на атакуемом объекте

без обратной связи (однонаправленная атака) – атака, в ходе реализации которой не требуется реагировать на изменения на атакуемом объекте. Такие атаки обычно осуществляются при помощи передачи на атакуемый объект одиночных запросов.

Воздействие на ИС может начать осуществляться только при определенных условиях. Существуют три вида таких условий: атака по запросу от атакуемого объекта; атака по наступлению ожидаемого события на атакуемом объекте; безусловная атака.

Воздействие со стороны атакующего начнется при условии, что потенциальная цель атаки передаст запрос определенного типа. Такую атаку можно назвать атакой по запросу от атакуемого объекта. Данный тип атак наиболее характерен для распределенных систем. Примером подобных запросов в сети Интернет может служить DNS- и ARP-запросы.

Атака по наступлению ожидаемого события на атакуемом объекте. Атакующий непрерывно наблюдает за состоянием ОС удаленной цели атаки и начинает воздействие при возникновении конкретного события в этой системе. Атакуемый объект сам является инициатором начала атаки. Примером такого события может быть прерывание сеанса работы пользователя с сервером.

Безусловная атака осуществляется немедленно и безотносительно к состоянию операционной системы и атакуемого объекта. Следовательно, атакующий является инициатором начала атаки в данном случае.

По расположению субъекта атаки относительно атакуемого объекта:

внутрисегментное;

межсегментное.

Во время внутрисегментной атаки субъект и объект атаки располагаются в одном сегменте. В случае межсегментной атаки субъект и объект атаки находятся в разных сетевых сегментах. Этот классификационный признак дает возможность судить о так называемой «степени удаленности» атаки.

Прежде чем рассматривать различные виды атак, разберем в вкратце общий процесс атаки. Существует несколько различных этапов, которые составляют атаку на компьютер или сеть, начиная с первоначальной мотивации, до окончательного выполнения атаки.

В целом есть четыре основных этапа:

мотивация и цели атакующего;

сбор информации / выбор цели;

выбор атаки;

выполнение атаки;

удаление следов.

У атакующего может быть много разных причин для запуска атаки. Некоторые атакующие могут просто хотят проверить свои навыки, другие могут преследовать конкретные цели. Мотивация влияет на то, какие способы осуществления атаки выбраны и как они выполняются.

Перед запуском атаки атакующий должен выбрать цель и собрать о ней информацию. Эти два этапа могут проходить одновременно или последовательно, в зависимости от того, чего хочет достичь атакующий. Сбор информации включает в себя извлечение полезной информации (в том числе уязвимостей) из целевой сети или хоста путем сканирования сети.

Как только выбрана цель и собрана какая-то информация о потенциальных недостатках (уязвимостях) цели, можно выбирать подходящий сценарий атаки. Следующий этапом является выполнение атаки, в которой атакующий начинает атаку против цели. На заключительном этапе отчищаются журналы аудита или заполняются ложными записями.

Для осуществления вредоносного воздействия на ИС могут быть использованы следующие разновидности ВПО и компьютерных атак: вирусы; черви; трояны; переполнение буфера; отказ в обслуживании; удаленные сетевые атаки; физические (локальные) атаки; парольные атаки; атаки сбора информации (сетевой анализ); социальная инженерия; комбинированные атаки.

Рассмотрим указанные виды ВПО и вредоносного воздействия более подробно.

1. *Вирусы.* Являются самовоспроизводящими программами, которые распространяются, заражая файлы. Они прикрепляются к файлу, что приводит к их запуску при открытии файла. Существует несколько основных типов вирусов.

1.1. *Файловые вирусы.* Заражают файлы на компьютере жертвы, внедряясь в исполняемые файлы (*.exe, *.com или *.bat) в ОС Windows.

1.2. *Вирусы системные (загрузочные).* Являлись наиболее распространенным типом вируса до середины 1990-х годов. Эти типы вирусов способны инфицировать базовую загрузочную запись жесткого диска (MBR)

либо иного МНИ, после чего могут запускаться каждый раз при загрузке СВТ, не попадая при этом в поле зрения антивирусной программы.

1.3. *Макровирусы.* По сути, это макросы для программ типа Microsoft Word и Microsoft Excel, которые являются вредоносными (например, они могут удалять информацию из документа или искажать ее). Распространение обычно происходит через зараженные файлы: если пользователь открывает зараженный документ, вирус может установить себя так, чтобы все последующие документы также были заражены.

Вирусы могут быть многосоставными, скрытыми, зашифрованными или полиморфным. Многосоставные вирусы представляют собой гибридные вирусы, которые заражают как файлы, так и системные и/или загрузочные записи. Скрытые вирусы пытаются скрыть свое присутствие в системе путем внедрения в файлы. Некоторые вирусы используют шифрование основной части своего кода, дешифруя ее только при запуске. Это позволяет им скрывать свою вредоносную сущность от антивирусной программы свою вредоносную сущность, их сложнее обнаружить и проанализировать.

Некоторые вирусы спустя определенное время способны модифицировать свой код, это дает им возможность маскировать свою деструктивную направленность. Такие вирусы называются полиморфными.

2. *Черви.* Представляют собой ВПО, которое каким-либо образом распространяется по сети. В отличие от обычных вирусов, черви не требуют распространения зараженного файла. Существует два основных типа червей: почтовые черви и сетевые черви.

2.1. *Почтовые черви* рассылаются по сети в виде приложений к сообщениям электронной почты. Это может быть копия самого червя или ссылка на файл, размещенный на вредоносном веб-ресурсе. Для активации полученного кода нужно открыть полученный файл или нажать на ссылку для перехода.

2.2. *Сетевые черви* представляют собой тип вредоносных программ, способных распространяться как по ЛВС, так и в сети Интернет, создавая свои копии. В отличие от файловых вирусов, сетевые черви могут использовать для размножения сетевые протоколы и устройства. Попадая в СВТ, они отправляют

по сети копии самого себя на машины других пользователей. По форме существования сетевые черви бывают обычными и пакетными. Обычные, проникая в систему через МНИ или сеть Интернет, воспроизводят себя в большом количестве, а затем рассылают эти дубли по электронным адресам, найденным на компьютере, или распределяют их по папкам общего доступа в локальной сети. Пакетные черви существуют в виде особого сетевого пакета; внедрившись в устройство, они стремятся проникнуть в его оперативную память с целью сбора информации (логины, пароли, содержимое буфера обмена и пр.).

3. *Трояны.* Разновидность ВПО, проникающая в компьютер под видом легитимного ПО, в отличие от вирусов и червей, которые распространяются самопроизвольно. В данную категорию входят программы, осуществляющие различные неподтверждённые пользователем действия: сбор информации о хосте, передача этой информации злоумышленнику, а также использование, удаление или злонамеренное изменение, нарушение работоспособности СВТ, использование его ресурсов в целях майнинга, нелегальной торговли и т.п.

4. *Логические бомбы.* Особый вид троянов, которые только освобождают свою полезную нагрузку после наступления определенного условия или события. Например, логическая бомба может сработать в определенное время. Если условие не выполняется, логическая бомба ведет себя как полезная программа.

5. *Переполнение буфера.* Является наиболее распространенным средством вредоносной атаки на компьютер или сегмент сети. Эта атака редко запускаются сама по себе, обычно являются частью смешанной атаки. Переполнение буфера использует ошибки в алгоритмах, в которых буферы разрешены для переполнения. Если буфер заполнен сверх его возможностей, данные, заполняющие его, могут затем переполняться в соседнюю память, а затем могут либо повреждать данные, либо использоваться для изменения исполнения программы.

6. *Отказ в обслуживании.* Атаки класса «Отказ в обслуживании» (DoS) предназначены для того, чтобы лишить законных пользователей ИС доступа или возможности нормальной работы с ИС. Подобные вредоносные атаки

обычно нарушают нормальное функционирование услугу сети, сетевых ресурсов или компьютера либо полностью их блокируют.

7. *Удаленные сетевые атаки.* Способов реализации удаленных сетевых атак несколько. К ним можно отнести подмену доверительного узла сети (Spoofing); захват сеанса; беспроводные сетевые атаки; атаки веб-приложений.

7.1. *Подмена доверительного узла сети.* Процесс, в котором атакующий выдает себя за другого пользователя. Существует несколько способов подмены в стандартном стеке сетевых протоколов TCP/IP, включая: спуфинг MAC-адресов на уровне канала передачи данных (MAC-Spoofing) и IP-спуфинг на сетевом уровне (IP-Spoofing).

7.1.1. *MAC-Spoofing.* Метод изменения MAC-адреса сетевого устройства, позволяющий обойти список контроля доступа к серверам, маршрутизаторам, либо скрыть компьютер, что может нарушить работоспособность сети.

7.1.2. *IP-Spoofing*. Вид вредоносной атаки, заключающийся в использовании чужого IP-адреса источника с целью обмана системы безопасности. Состоит в изменении поля «адрес отправителя» IP-пакета. Применяется с целью сокрытия истинного адреса атакующего, с целью вызвать ответный пакет на нужный адрес.

7.2. *Захват сеанса (сессии).* Атака на идентификаторы сеансов пользователей сети Интернет с целью получения контроля над веб-сеансами. Включает в себя отправку поддельных сообщений, которые отвечают «да, я – это вы». Позволяет осуществлять НСД к информации или службам в ИС.

7.3. *Беспроводные сетевые атаки.* Эксплуатируют уязвимости беспроводных сетей, в которых существует ряд недостаточно защищенных областей, не свойственных традиционным проводным сетям. Например, большинство беспроводных сетей требуют только подтверждения MAC-адресов для получения полного доступа.

7.4. *Атаки веб-приложений*. Разновидность сетевой атаки, направленная на веб-приложения. По сути, вредоносным воздействиям подвергается уровень приложений стека протоколов TCP/IP. Атаки веб-приложений отличаются от атак, которые нацелены на обычные приложения тем, что используют сетевые протоколы. Ниже описано несколько основных способов, с помощью которых

злоумышленник способен атаковать веб-приложения.

7.4.1. *Внедрение скрипта для сайта.* Скрипт – это программный код (сценарий), написанный на JavaScript и PHP (как правило). Вредоносные скрипты, которые встраиваются в код веб-страниц, интерпретируются браузером пользователя и выполняют действия, заложенные злоумышленниками (например, захват сетевого сеанса, перенаправление на фишинговые веб-страницы, попытка майнинга криптовалюты в веб-браузере, отображение рекламы с целью накруток, хищение персональных данных и др.).

7.4.2. *Подмена параметров*. Атака веб-приложения, в которой атакующий идентифицирует параметры, используемые для управления веб-приложением, и изменяет заголовок URL-адреса для управления параметрами. Позволяет осуществить НСД в хранимым на атакуемом сайте данных.

7.4.3. *SQL-инъекция*. Общее наименование группы атак, позволяющих злоумышленнику производить различные несанкционированные действия над базой данных. Они могут затрагивать как сами данные, так и структуру базы. Для этого в качестве входных данных передаются специальные строки, содержащие вредоносные команды. Веб-приложение, уязвимое к SQL-инъекциям, производит вставку этих строк в шаблон запроса без проведения необходимых проверок. В результате формируется запрос, выполняющий действия, определённые злоумышленником. При этом с точки зрения синтаксиса SQL запрос будет являться корректным.

7.4.4. *Скрытая манипуляция полем.* Механизм этой атаки заключается в следующем: атакующий загружает HTML-страницу и изменяет скрытые поля, расположенные на странице и содержащие важные пользовательские данные (например, идентификаторы сеанса). Затем атакующий перенаправляет страницу на вредоносный сервер.

8. *Физические атаки.* Одна из форм реализации атаки на СВТ, состоящей в физическом воздействии на объект доступа (подбор паролей, использование ошибок в ПО, модификация программного кода, восстановление хешированных паролей, внедрение клавиатурного шпиона с целью получить контроль над компьютером или учетной записью пользователя и пр.).

8.1. *Атаки брутфорса*. Представляют собой способ подбора паролей к

ИС, в котором для получения хешированных паролей используются автоматически генерируемые последовательности символов, т. е. перебираются их всевозможные комбинации до тех пор, пока пароль не будет подобран. При этом обычно учитывается наименьшая и наибольшая возможная длина пароля.

8.2. *Атака «Подбор пароля по словарю».* Атака на систему защиты ИС, использующая метод полного перебора предполагаемых паролей, используемых для аутентификации, осуществляемого путём последовательного пересмотра всех слов (паролей в чистом виде или их зашифрованных образов – хэшей) определённого вида и длины из словаря с целью последующего взлома системы и получения доступа к защищаемой информации.

8.3. *Превышение полномочий.* Разновидность физической вредоносной атаки, используемой ошибки в ПО или в администрировании ОС. При этом осуществляется запуск программы от имени пользователя, имеющего необходимые полномочия, или в качестве системной программы (драйвера, сервиса и т. д.). Могут проводится подмена динамически загружаемой библиотеки, используемой системными программами, изменение переменных среды, описывающих путь к таким библиотекам, несанкционированная модификация кода или данных подсистемы зашиты самой ОС.

9. *Атаки на сбор информации (первоначальная разведка среды).* Сбор информации – это процесс, с помощью которого атакующий получает ценную информацию о потенциальных целях или получает неавторизованный доступ к некоторым данным без запуска атаки. Сбор информации является пассивным видом атаки в том смысле, что атаки не запускаются явно. Вместо этого сети и компьютеры сканируют, проверяют и исследуют информацию.

9.1. *Пакетные снифферы.* Представляют собой ПО или аппаратные средства, предназначенные для перехвата и/или анализа сетевого трафика. Обеспечивают сбор информации об атакуемых хосте или пользователе, а также получение НСД к целевой информации.

Таким образом, с учетом выявляемых угроз ИБ ИС режим защиты должен формироваться как совокупность способов и мер защиты циркулирующей в ИС информации и поддерживающей её инфраструктуры от случайных или преднамеренных воздействий естественного или

искусственного характера, влекущих за собой нанесение ущерба владельцам или пользователям информации и поддерживающей инфраструктуры;

система обеспечения ИБ ИС должна предусматривать комплекс организационных, программных и технических средств и мер по защите информации в процессе её обработки и хранения (как при передаче информации по каналам связи, так и при ведении конфиденциальных переговоров, раскрывающих сведения с ограниченным доступом);

защиту информации в ИС следует осуществлять на всех этапах жизненного цикла ее обработки при комплексном использовании всех имеющихся средств защиты, объединенных в единый целостный механизм. Это позволит максимально эффективно обеспечить целостность и конфиденциальность обрабатываемой информации при условии ее доступности для пользователей, имеющих соответствующие права.

2.3. Способы и средства защиты информации от утечки по техническим каналам

Неотъемлемым условием построения эффективной системы защиты информации ограниченного распространения является всестороннее изучение объекта защиты. Крайне важным представляется получение достоверных оценок уровня его защищенности, определение возможных путей организации НСД к циркулирующей в нем информации, обнаружение вероятных ТКУИ и постоянный их мониторинг.

Существующие методы обнаружения ТКУИ основываются на использовании специальных технических средств и предполагают активный либо пассивный способы поисковых работ.

При *активном типе обнаружения ТКУИ* могут быть использованы следующие технические устройства:

нелинейные локаторы (реагируют на наличие электромагнитного поля);

рентгенметры (осуществляют вычисление ТКУИ путем просвечивания с помощью рентгеновских излучений).

магнитно-резонансные локаторы (выявляют посторонние вмешательства по молекулам в магнитном поле);

цифровые акустические корреляторы (определяют наличие закладных устройств в металлоконструкциях).

Пассивный способ обнаружения ТКУИ осуществляется с помощью:

металлоискателей (электронные приборы, позволяющие обнаруживать металлические предметы в нейтральной или слабо-проводящей среде за счёт их проводимости. Способны обнаруживать металлические предметы в грунте, воде, стенах, в древесине, под одеждой, в багаже, в пищевых продуктах, в организме человека и животных и т. д.);

тепловизоров (устройства, принцип действия которых основан на выделении тепла любым техническим устройством. Обладают высокой чувствительностью, способны регистрировать сигналы мощностью 1 мкВт);

приборов по изменению всех показателей телефонной линии (индукции, напряжения, емкости), которые позволяют обнаруживать устройства съема информации на основе индукционных датчиков;

анализаторов спектра и измерителей частот (позволяют выявлять радиозакладные устройства широкого спектра);

детекторов видеокамер (способны обнаруживать скрытно установленные видеокамеры).

Общим для всех перечисленных устройств является то, что их задача состоит в выделении сигнала передатчика.

Нередко злоумышленники используют тщательно замаскированные закладные аудио-видеоустройства, помещая их в корпус бытовых предметов (часы, зеркало, настольная лампа и пр.). Такие закладки можно обнаружить лишь при их разборке либо просвечивании рентгеновскими лучами.

При выявлении ТКУИ рекомендуется обращать внимание на следующие демаскирующие признаки закладных устройств:

наличие в служебном помещении выходящего наружу тонкого провода непонятного назначения. Он может быть подсоединен к небольшому закамуфлированному микрофону;

присутствие в рабочем помещении посторонних малогабаритных предметов, снабженных аккумуляторными батареями, а также бытовых предметов с нехарактерными отверстиями в корпусе;

расход тока при полностью отключенных рабочих приборах (заметный по показаниям электросчетчика);

нетипичные показания емкости в линии подачи электроэнергии после ее отключения от источника питания (на щитке).

При выявлении ТКУИ необходимо рассматривать всю совокупность технического оборудования ИС, включающую ТСОИ, оконечные устройства (принтеры и сканеры, видеокамеры локальных систем видеонаблюдения, POS-терминалы и т. п.), соединительные линии, распределительные и коммутационные устройства, системы электропитания (стабилизаторы, источники бесперебойного питания и пр.), системы заземления и т. д. Следует учитывать и наличие на защищаемом объекте ВТСС (оборудование открытой

телефонной, факсимильной, громкоговорящей связи, системы охранной и пожарной сигнализации, электрификации и радиофикации, электробытовые приборы и др.). Существенную роль при формировании ТКУИ играют выходящие за пределы КЗ разнообразные технические средства, а также посторонние провода, металлические трубы систем отопления и водоснабжения, различные токопроводящие металлоконструкции, проходящие через помещения, где установлены основные и вспомогательные технические средства.

Необходимо отметить, что для возникновения технических КУИ необходимы определенные пространственные, энергетические и временные условия, а также соответствующие средства выделения информации из сигнала или носителя, ее восприятия и фиксации на стороне злоумышленника. Определяющее значение имеет и месторасположение средства выделения информации из сигнала или носителя, которое может быть в пределах КЗ, охватывающей ИС, либо вне ее.

Инженерно-техническая защита информации ограниченного распространения, обрабатываемой в ИС, предполагает комплекс мероприятий по защите информации от НСД по различным ТКУ, а также нейтрализацию специальных воздействий на нее – уничтожения, искажения или блокирования доступа. Рассмотрим некоторые подходы к методологии такой защиты.

Методы устранения акустических ТКУИ основываются на физических процессах, лежащих в основе функционирования средств несанкционированного съема информации по данным каналам – процессах распространения акустических волн в твердых однородных средах (к ним относятся различные строительные конструкции зданий и сооружений, коммуникации водоснабжения и отопления, и т. п.). Указанные методы предполагают использование двух подходов.

Первый из них – это метод пассивной акустической изоляции, основанный на использовании в защищаемых помещениях специальных рассеивателей и поглотителей звуковой волны (акустических демпферов).

Второй метод реализует активное акустическое и виброакустическое зашумление с помощью специальных генераторов низкочастотных (звуковых)

шумовых акустических и виброакустических сигналов, которые предназначены для акустического и виброакустического зашумления каналов утечки информации.

Защита от прямого акустического снятия информации основывается на выявлении и устранении строительных дефектов и изъянов с точки зрения ухудшения звукоизоляции: устраняются дефекты в стенах и перекрытиях, встраивается дополнительная звукоизоляция в виде фальшпотолков, фальшстен, акустических и виброакустических экранов, устанавливаются специальные оконные рамы на основе вакуумного застекления.

Для защиты речевых сигналов от несанкционированного снятия по виброакустическим каналам утечки информации могут быть использованы методы активного виброакустического зашумления. Их суть заключается в наведении в строительных конструкциях служебных зданий и сооружений упругих шумовых виброколебаний, распространяющихся по всему объему строительной конструкции, вызывая шумовые микродеформации. Последние, в свою очередь, подавляют микродеформации, создаваемые воздействием речевых сигналов на те же конструкции, т. е. происходит шумовое виброзашумление упругих волн, создаваемых речевыми сигналами людей, находящихся в КЗ. В результате существенно снижается возможность восприятия речевых сигналов, а также их перехвата устройствами несанкционированного съема.

Система виброакустического зашумления состоит из генератора низкочастотных шумовых сигналов, нескольких вибропреобразователей, осуществляющих формирование виброакустических сигналов.

Датчики вибропреобразователей виброакустического зашумления в случае стационарного оборудования объекта защиты монтируются на перекрытиях, стенах, водопроводных коммуникациях и отопительных батареях, вентиляционных шахтах, оконных переплетах и т. д., и создают заградительную виброакустическую помеху в элементах строительных конструкций.

Во время отсутствия в контролируемых помещениях звуковых сигналов вибродатчики находятся в режиме «молчания», при появлении в

контролируемых помещениях звуковых сигналов акустические микрофоны воспринимают их и вырабатывают команду для включения шумовых вибропреобразователей.

Для подавления устройств несанкционированной записи речевой информации (диктофонов) используются устройства электромагнитного подавления. Принцип их действия заключается в генерации импульсных высокочастотных шумовых сигналов, воздействующих на элементы электрической схемы записывающего устройства (в частности, усилители низкой частоты) и вызывающих в них наводки шумовых сигналов. Это приводит к тому, что при несанкционированной записи наряду с полезным речевым сигналом записывающим устройством будет записан и сгенерированный шум, интенсивность и частота которого существенно перекроет полезный сигнал.

Защита информации от утечки через электротехнические ТКУИ также осуществляется с применением пассивных и активных методов и средств. Общей целью указанных методов защиты является уменьшение отношения *сигнал / шум* на границе КЗ до величин, обеспечивающих невозможность выделения средством технической разведки злоумышленника полезного информационного сигнала. В пассивных методах защиты уменьшение отношения сигнал / шум достигается путем уменьшения уровня опасного сигнала, в активных методах – путем увеличения уровня шума.

Пассивные методы защиты информации направлены на:

ослабление ПЭМИН в технических устройствах, функционирующих как в пределах границ КЗ, так и выходящих за ее пределы;

исключение (ослабление) просачивания информационных сигналов в цепи электропитания и заземления, выходящие за пределы КЗ.

Ослабление информативного сигнала следует проводить до величин, обеспечивающих невозможность его выделения средством технической разведки на фоне естественных шумов.

К пассивным методам защиты относятся:

применение разделительных трансформаторов и помехоподавляющих фильтров;

экранирование;

заземление всех технических средств;

доработка устройств СВТ с целью минимизации уровня излучения.

Активные методы защиты информации направлены на:

создание маскирующих пространственных электромагнитных помех;

создание маскирующих электромагнитных помех в ВТСС.

К активным методам защиты относятся пространственное и линейное зашумление.

Пространственное зашумление осуществляется за счет прицельного излучения электромагнитных сигналов в окружающее пространство. Применяется для защиты от ПЭМИН как конкретного элемента ИС, так и для защиты всего объекта. Несмотря на то, что этот метод направлен на обеспечение невозможности выделения ПЭМИН на фоне создаваемых помех во всех диапазонах излучения, уровень создаваемых помех не должен превышать санитарных норм и норм по электромагнитной совместимости радиоэлектронной аппаратуры.

При использовании линейного зашумления генераторы прицельных помех подключаются к токопроводящим линиям для создания в них электрических помех, которые не позволяют злоумышленникам выделять наведенные сигналы.

Защита информации от угроз, создаваемых в результате возникновения *физических КУИ* реализуется путем осуществления организационных (административных) мероприятий. Такие мероприятия направлены на решение многочисленных вопросов регламентации взаимодействия работников с техническими средствами и между собой, процессов функционирования системы обработки данных и использование ее ресурсов с тем, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

Организационные меры включают следующие ключевые аспекты:

разработка правил доступа пользователей к ресурсам ИС (политики безопасности);

работа с персоналом, его подбор и расстановка, включая ознакомление с сотрудниками, их изучение, обучение правилам работы с конфиденциальной информацией, ознакомление с мерами ответственности за нарушение правил защиты информации и т. д.;

организация охраны и надежного пропускного режима, исключающего возможность тайного проникновения на территорию и в помещения посторонних лиц.

Основная цель мер организационного уровня – определить стратегию защиты и сформировать программу работ в области ИБ, обеспечить ее выполнение. Основой такой программы является **политика безопасности –** *совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.*

Вопросы обеспечения ИБ в контексте нейтрализации *информационных КУИ* разрешаются в рамках организации работы подсистем безопасности ОС, составляющих основу программно-аппаратного обеспечения защищаемых СВТ, а также иных методов и средств защиты информации, обрабатываемой ИС. Интенсивное развитие современных информационных технологий, все более широкое их использование в деятельности ОВД придает особую актуальность задаче постоянного совершенствования системы защиты ведомственных информационных ресурсов.

В настоящее время в ОВД проводится интенсивная работа по модернизации ведомственной системы ИБ, основывающейся на качественно новых подходах. Так, приказом Министерства внутренних дел Республики Беларусь «О единой цифровой платформе Министерства внутренних дел» № 256 от 30.09.2022 утверждены входящие в состав документированной информации в области обеспечения ИБ, следующие нормативно–методические документы:

политика ИБ единой цифровой платформы Министерства внутренних дел;

инструкция по обеспечению защиты информации единой цифровой платформы Министерства внутренних дел;

инструкция по определению парольной политики и организации порядка доступа к отдельному сегменту ведомственной сети передачи данных органов внутренних дел;

регламент защиты от вредоносного программного обеспечения единой цифровой платформы Министерства внутренних дел;

регламент криптографической защиты информации единой цифровой платформы Министерства внутренних дел;

регламент межсетевого экранирования единой цифровой платформы Министерства внутренних дел;

регламент мониторинга, аудита событий ИБ и реагирования на инциденты ИБ единой цифровой платформы Министерства внутренних дел;

регламент резервирования и уничтожения информации единой цифровой платформы Министерства внутренних дел.

Объектами защиты информации в компьютерных системах ЕЦП являются:

информация, хранящаяся и обрабатываемая в ИС;

ИС, содержащие информацию ограниченного распространения.

В рамках обеспечения ИБ в ОВД используется **многоуровневая модель деления уровней функционирования ИС**, включающая:

уровень сбора событий, на котором проводится сбор событий аудита и событий, связанных с состоянием инфраструктуры ЕЦП;

организационный уровень, на котором проводится разработка локальных правовых актов, регламентирующих функционирование ИС, методических рекомендаций, обучение и консультации субъектов информационных отношений ЕЦП по работе в соответствующей информационной среде;

прикладной уровень, на котором проводится установка и обновление прикладного ПО для ЕЦП, администрирование субъектов информационных отношений ЕЦП, контроль доступа к ЕЦП;

уровень баз данных, на котором проводится настройка, управление, резервное копирование и восстановление баз данных, контроль работоспособности систем управления баз данных;

системный уровень, на котором проводится установка и настройка систем управления базами данных (включая создание требуемых объектов, таблиц и др.), серверов приложений, иного системного ПО, необходимого для функционирования ЕЦП ОВД, установка и обновление ОС, драйверов;

сетевой уровень, на котором проводится организация линий связи и каналов передачи данных, выделение IP–адресов, маршрутизация трафика, настройка правил доступа, сетевого оборудования, обновление встроенного ПО и сетевого оборудования;

физический уровень, на котором обеспечивается энергоснабжение, кондиционирование, исправность серверного и коммутационного оборудования, ограничение доступа в серверные помещения.

Субъектами информационных отношений при обеспечении ИБ ЕЦП являются:

Министерство внутренних дел Республики Беларусь – в качестве обладателя активов ЕЦП;

государственные органы и организации, юридические лица – в качестве пользователей активами ЕЦП в рамках договоров (положений о взаимодействии, соглашений, регламентов);

иные юридические лица – в качестве операторов ИС и связи, поставщиков ПО, комплекса программно–технических средств и средств комплексной защиты информации, и (или) в качестве оказания МВД услуг технической поддержки, и (или) осуществляющие гарантийное и сервисное обслуживание.

В сфере информационных отношений в МВД выделяют следующие категории пользователей:

внутренние пользователи, к которым относятся:

сотрудники подразделения контроля обеспечения ИБ ЕЦП[1], осуществляющие контроль выполнения внутренними пользователями требований законодательства, настоящей Политики и ее состояния, а также иных правовых актов;

[1] отдел (контроля обеспечения ИБ) управления оперативно–аналитической работы и контроля обеспечения ИБ ГУСБ, отделы оперативно–аналитической работы и контроля обеспечения ИБ территориальных управлений ГУСБ

сотрудники подразделений по защите информации, осуществляющие организацию и обеспечение безопасного функционирования активов ЕЦП;

руководители структурных подразделений ОВД, принимающие меры по обеспечению сохранности защищаемой информации в подотчетных подразделениях, в обслуживаемых ИС, в отношении подчиненных сотрудников;

сотрудники, назначенные владельцами ИС, обеспечивающие их безопасное функционирование, в том числе по предоставлению доступа пользователям;

сотрудники, получившие доступ к активам ЕЦП и использующие их в рамках выполнения своих должностных обязанностей;

внешние пользователи, к которым относятся:

работники сторонних организаций, использующие ЕЦП в рамках выполнения своих функциональных обязанностей;

должностные лица организаций, поставляющие активы для ЕЦП и осуществляющие их гарантийное и сервисное обслуживание;

иные физические и юридические лица, использующие активы ЕЦП в установленном порядке.

Для обслуживания и сопровождения системы защиты информации ЕЦП используется ролевая модель, в соответствии с которой уполномоченным лицам по обеспечению ИБ ЕЦП могут определяться следующие роли:

аудитор ИБ, на роль которого определяются сотрудники подразделений по защите информации. Аудиторы ИБ должны иметь высшее образование в области защиты информации, либо высшее или профессионально–техническое образование с последующей переподготовкой или повышением квалификации по вопросам технической и комплексной защиты информации в порядке, установленном законодательством;

администратор ИБ, на роль которого определяются сотрудники подразделений по защите информации, уполномоченные лица, ответственные за обеспечение ИБ;

администратор ИБ ИС, на роль которого определяются сотрудники подразделений по защите информации, уполномоченные лица, ответственные за обеспечение ИБ ИС.

Внутренние пользователи в пределах, предоставленных им прав и (или) полномочий имеют право использовать ЕЦП для доступа к ИС с целью поиска, получения, передачи, сбора, обработки, накопления, хранения, распространения, предоставления и (или) получения информации, а также осуществлять иные действия в соответствии с должностными инструкциями и локальными правовыми актами Министерства внутренних дело.

Внутренние пользователи ЕЦП обязаны:

соблюдать возложенные на них обязанности в соответствии с положениями о структурных подразделениях, иными правовыми актами, должностными инструкциями;

принимать меры по защите информации;

обеспечивать сохранность информации, распространение и (или) предоставление которой ограничено, полученной в результате доступа в рамках исполнения своих должностных обязанностей;

использовать активы ЕЦП в пределах предоставленных прав;

соблюдать требования документации, разработанной для ИС ЕЦП;

незамедлительно сообщать обо всех нетипичных поведениях (событиях, инцидентах, угрозах, уязвимостях и так далее) ЕЦП и ее системы защиты информации.

В рамках реализации деятельности по обеспечению ИБ ЕЦП уполномоченными лицами по обеспечению ИБ ЕЦП осуществляются:

оценка важности информационных активов;

выявление угроз ИБ;

мониторинг факторов риска ИБ и соответствующий их пересмотр;

управление рисками ИБ;

управление инцидентами ИБ, включающее в себя мониторинг, выявление и анализ инцидентов ИБ, оперативное реагирование на них и последующее их расследование;

учет подлежащих защите ИС;

сбор информации о событиях ИБ;

минимизация негативных последствий инцидентов ИБ;

оперативное доведение до руководства Министерства внутренних дел информации о наиболее значимых инцидентах ИБ и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты ИБ;

взаимодействие с компетентными органами безопасности по выявленным инцидентам ИБ;

выполнение принятых решений по всем инцидентам ИБ в установленные сроки;

пересмотр применяемых требований, мер и механизмов по обеспечению ИБ по результатам рассмотрения инцидентов ИБ;

мероприятия по повышению уровня знаний сотрудников подразделений по защите информации, уполномоченных лиц, ответственных за ИБ ИС;

обеспечение регламентации и управления доступом к активам;

обеспечение бесперебойной работы автоматизированных систем и сетей передачи данных;

обеспечение возобновления работы автоматизированных систем и сетей передачи данных после прерываний и нештатных ситуаций;

применение средств защиты от ВПО;

обеспечение ИБ на всех стадиях жизненного цикла автоматизированных систем МВД, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием).

Реализация технической политики в области обеспечения ИБ ИС должна исходить из предпосылки, что невозможно обеспечить требуемый уровень защищенности информации не только с помощью одного отдельного средства (мероприятия), но и с помощью их простой совокупности. Необходимо их взаимное согласование между собой (комплексное применение), а отдельные разрабатываемые элементы информационной системы должны рассматриваться как часть единой ИС в защищенном исполнении при оптимальном соотношении технических (аппаратных, программных) средств и организационных мероприятий.

Основными направлениями реализации технической политики обеспечения ИБ ИС являются:

обеспечение защиты информационных ресурсов от хищения, утраты, утечки, уничтожения, искажения или подделки за счет НСД;

обеспечение защиты информации от утечки по ТКУИ при её обработке, хранении и при передаче по каналам связи.

В рамках указанных направлений технической политики обеспечения ИБ осуществляются:

реализация разрешительной системы допуска исполнителей (пользователей, обслуживающего персонала) к работам, документам и информации конфиденциального характера;

реализация системы инженерно-технических и организационных мер охраны, предусматривающей многорубежность и равнопрочность построения охраны (территории, здания, помещения) с комплексным применением современных технических средств охраны, обнаружения, наблюдения, сбора и обработки информации, обеспечивающих достоверное отображение и объективное документирование событий;

ограничение доступа исполнителей и посторонних лиц в здания и помещения, где проводятся работы конфиденциального характера и размещены средства информатизации и коммуникации, на которых обрабатывается (хранится, передается) информация ограниченного распространения, непосредственно к самим средствам информатизации и коммуникациям;

разграничение доступа пользователей и обслуживающего персонала к информационным ресурсам, программным средствам обработки (передачи) и защиты информации в подсистемах различного уровня и назначения, входящих в АС;

учет документов, информационных массивов, регистрация действий пользователей и обслуживающего персонала, контроль НСД и действий пользователей, обслуживающего персонала и посторонних лиц;

предотвращение внедрения в автоматизированные подсистемы программ-вирусов, программных закладок и т.п.

криптографическое преобразование информации, обрабатываемой и передаваемой средствами вычислительной техники и связи;

надежное хранение традиционных и МНИ, а также их обращение, исключающее хищение, подмену и уничтожение;

необходимое резервирование технических средств и дублирование массивов и носителей информации;

снижение уровня и информативности побочных электромагнитных излучений и наводок (ПЭМИН), создаваемых различными элементами ИС;

обеспечение акустической защиты помещений, в которых обсуждается информация конфиденциального характера;

электрическая развязка цепей питания, заземления и других цепей объектов информатизации, выходящих за пределы КЗ;

активное зашумление в различных диапазонах;

противодействие оптическим и лазерным средствам наблюдения.

ГЛАВА 3.

АППАРАТНОЕ И ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ЗАЩИЩЕННЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

3.1. Операционные системы и их защищенность

Для решения стоящих перед ОВД задач реализуется комплекс мер, направленных на совершенствование ЕЦП на основе оснащения их современными техническими комплексами, внедрения в практическую деятельность новых и перспективных информационных технологий. С другой стороны, активное развитие информационных и телекоммуникационных технологий в деятельность ОВД неотрывно связано с ее защитой и обеспечением ИБ.

Наиболее доступными и уязвимыми компонентами ИС являются рабочие СВТ – автоматизированные рабочие места пользователей. Именно с них могут быть предприняты наиболее многочисленные попытки НСД и попытки совершения несанкционированных действий (непреднамеренных и умышленных). С рабочих СВТ осуществляется управление процессами обработки информации (в том числе на серверах), запуск программ, ввод и корректировка данных, на жестких дисках СВТ могут размещаться критически важные данные и программы обработки. На мониторы и печатающие устройства СВТ выводится информация при работе пользователей, выполняющих различные функции и имеющих разные полномочия по доступу к данным и другим ресурсам системы. Нарушения конфигурации аппаратно-программных средств СВТ и неправомерное вмешательство в процессы их функционирования могут приводить к блокированию информации,

невозможности своевременного решения важных задач и выходу из строя отдельных СВТ и подсистем ИС.

В особой защите нуждаются такие элементы ЛВС как выделенные файловые серверы, серверы баз данных и серверы приложений. Здесь злоумышленники, прежде всего, могут искать возможности получения доступа к защищаемой информации и оказания влияния на работу различных подсистем серверов, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам серверов. При этом могут предприниматься попытки как удаленного (с использованием СВТ, подключенных к сети) так и непосредственного (например, с консоли сервера) воздействия на работу серверов и их средств защиты.

Проблема защиты от вышеуказанных несанкционированных действий может быть успешно решена только на основе комплексной защиты ИС. Базовым средством многоуровневой комплексной защиты ИС от широкого спектра угроз, создаваемых информационными КУИ, является защищенная ОС. Это обусловлено тем, что именно ОС, с одной стороны – создает необходимые условия для формирования целого перечня уязвимостей для конкретных СВТ, входящих в состав ИС, а с другой – формирует основополагающие возможности для многоуровневой защиты обрабатываемой информации. Иными словами, уровень внутренней защищенности ОС напрямую влияет на состояние степень защиты ИС в целом.

Существуют несколько ключевых подходов к построению внутренней системы защиты ОС: фрагментарный и фундаментальный. Фрагментарный подход основывается на использовании разрозненных программных средств, как правило, от разных производителей, и функционирующих независимо друг от друга. Отдельные элементы подсистемы такой защиты практически не взаимодействуют друг с другом, поэтому могут некорректно работать на одной программно-аппаратной платформе. Это приводит к существенному снижению надежности системы.

Примером фрагментарного подхода может служить ситуация, когда за основу берется недостаточно незащищенная ОС (например, MS Windows XP),

на нее последовательно устанавливаются антивирусное ПО, система шифрования, сторонняя система протоколирования и аудита и т. п.

Наиболее эффективным является фундаментальный подход, при котором защитные функции внедряются в ОС еще на этапе проектирования архитектуры ОС и являются ее неотъемлемой частью. Отдельные элементы подсистемы защиты, созданной на основе фундаментального подхода, тесно взаимодействуют друг с другом при решении различных задач, связанных с организацией защиты информации, поэтому конфликты между ее отдельными компонентами практически невозможны. Подсистема защиты, созданная на основе фундаментального подхода, обычно устроена так, что при критических сбоях в функционировании ее ключевых элементов она вызывает крах ОС, но не позволяет злоумышленнику отключать защитные функции системы.

Для достижения основной цели защиты и обеспечения свойств защищенности информации ограниченного распространения и системы её обработки **система безопасности ИС должна обеспечивать эффективное решение следующих задач**:

защиту от вмешательства в процесс функционирования ИС посторонних лиц (возможность использования автоматизированной системы и доступ к её ресурсам должны иметь только зарегистрированные установленным порядком пользователи);

разграничение доступа зарегистрированных пользователей к аппаратным, программным и информационным ресурсам ИС (возможность доступа только к тем ресурсам и выполнения только тех операций с ними, которые необходимы конкретным пользователям ИС для выполнения своих служебных обязанностей), то есть защиту от НСД к информации, циркулирующей в ИС, рабочих СВТ, аппаратным, программным и криптографическим средствам защиты, используемым в ИС;

регистрацию действий пользователей при использовании защищаемых ресурсов ИС в системных журналах и периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов ответственными за ИБ;

контроль целостности (обеспечение неизменности) среды исполнения программ и её восстановление в случае нарушения;

защиту от несанкционированной модификации и контроль целостности используемых в ИС программных средств, а также защиту системы от внедрения ВПО;

защиту информации ограниченного распространения от утечки по ТКУ при её обработке, хранении и передаче по каналам связи;

защиту информации ограниченного распространения, хранимой, обрабатываемой и передаваемой по каналам связи, от несанкционированного разглашения или искажения;

обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

обеспечение живучести криптографических средств защиты информации при компрометации части ключевой системы;

своевременное выявление источников угроз ИБ, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений, создание механизма оперативного реагирования на угрозы ИБ и негативные тенденции.

С учетом необходимости выполнения вышеперечисленных задач реализация фундаментального подхода к построению архитектуры системы защиты ОС основывается на следующих основных подсистемах.

1.1. Доверенная загрузка

Предполагает загрузку различных ОС только с заранее определенных (доверенных) МНИ после успешного завершения специальных процедур: проверки целостности технических и программных средств СВТ (с использованием механизма пошагового контроля целостности), программной либо программно-аппаратной идентификации / аутентификации пользователя. Реализуется с помощью ***подсистемы BIOS*** *(Basic Input / Output System – базовая система ввода-вывода) – программы для первоначального запуска СВТ, настройки оборудования и обеспечения функций ввода-вывода.*

Все начальные загрузчики ОС обращаются к базовой системе ввода-вывода (BIOS) с тем, чтобы провести первоначальную инициализацию установленного оборудования и контрольное тестирование его работоспособности, а также получить сведения о том, каким образом выполнять дальнейшую загрузку ОС.

Поскольку ***BIOS*** *– это самый нижний уровень программного обеспечения, предназначенного для конфигурирования и управления оборудованием компьютера, в нем содержится код для взаимодействия со средствами ввода-вывода, дисковыми накопителями, коммуникационными портами и другими устройствами,* что с точки зрения ИБ можно рассматривать как серьезную уязвимость системы.

Учитывая, что BIOS запускается с высоким уровнем привилегий на ранней стадии загрузки системы, вредоносный код, исполняемый на уровне BIOS, достаточно трудно обнаружить. Кроме того, он может использоваться для повторного «инфицирования» системы даже после того, как была произведена переустановка ОС или даже замена жесткого диска компьютера.

В этих условиях BIOS и загрузчик воспринимаются нарушителем как привлекательные объекты атак:

атаки на BIOS, заключающиеся в подмене исходного кода BIOS вредоносным кодом BIOS, внедренным нарушителем;

атаки на загрузчик, заключающиеся в установке подконтрольного нарушителю так называемого «буткита» (bootkit, разновидность «руткита» (rootkit), который исполняется в режиме ядра), «инфицирующего» загрузчик. При этом «буткит» может использоваться для организации утечки чувствительной информации, обрабатываемой в процессе загрузки, такой как пароли шифрования информации на жестком диске.

Кроме того, изменив в BIOS приоритет носителя для первоочередной загрузки ОС, злоумышленник может загрузить ее со своего USB-носителя и с помощью специального вредоносного обеспечения осуществить сброс (обнуление) пароля от учетной записи, получив тем самым несанкционированный доступ к СВТ.

Для минимизации обозначенных угроз в BIOS предусмотрен ряд **настраиваемых опций безопасности**:

защита от случайного повреждения (обновления) BIOS пользователями или ВПО;

предупреждение при попытке обращения к загрузочному сектору или к таблице разделов жесткого диска;

режим защиты от записи для жесткого диска;

установление пароля администратора, который используется для запуска программы настройки BIOS или для запуска СВТ;

установление пароля пользователя, который используется для запуска программы настройки BIOS или для запуска СВТ (для изменения пароля необходимо зайти в систему с паролем администратора);

установление носителя для первоочередной загрузки ОС;

очередность загрузки ОС с жестких дисков (если их несколько);

порядок загрузки ОС с других устройств (МНИ);

контроль открытия корпуса СВТ, если он оборудован специальным датчиком;

управление утилитой S.M.A.R.T. (Self Monitoring Analysis and Reporting Technology), которая контролирует состояние жесткого диска, выявляет повреждения и по возможности устраняет их.

1.2. Идентификация, аутентификация и авторизация

С каждым зарегистрированным в ИС субъектом (пользователем или процессом, действующим от имени пользователя) связана некоторая информация, однозначно идентифицирующая его. Это может быть число или строка символов, именующие данный субъект. Эту информацию называют *идентификатором* субъекта. Если пользователь имеет идентификатор, зарегистрированный в сети, он считается легальным (законным) пользователем; остальные пользователи относятся к нелегальным пользователям. Прежде чем получить доступ к ресурсам ИС, пользователь должен пройти процесс первичного взаимодействия с компьютерной системой, который включает идентификацию, аутентификацию и авторизацию.

Идентификация *– это процедура распознавания пользователя по его идентификатору, присвоенному данному пользователю ранее и занесенному в базу данных в момент его регистрации в качестве легального пользователя системы.*

Эта функция выполняется в первую очередь, когда пользователь делает попытку войти в сеть. Пользователь сообщает системе по ее запросу свой идентификатор, и система проверяет в своей базе данных его наличие.

Аутентификация *– процедура проверки подлинности входящего в систему объекта (пользователя, процесса или устройства), предъявившего свой идентификатор.*

Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, не известную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация – *процедура предоставления пользователю (процессу или устройству) определенных прав доступа к ресурсам системы после успешного прохождения им процедуры аутентификации.*

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Администрирование *– это процесс управления доступом пользователей к ресурсам системы.*

С точки зрения обеспечения безопасности ОС, процедуры идентификации и аутентификации являются весьма ответственными. Действительно, если злоумышленник сумел войти в систему от имени другого пользователя, он

легко получает доступ ко всем объектам ОС, к которым имеет доступ этот пользователь. Если при этом подсистема аудита генерирует сообщения о событиях, потенциально опасных для безопасности ОС, то в журнал аудита записывается не имя злоумышленника, а имя пользователя, от имени которого злоумышленник работает в системе.

Наиболее распространенными **методами идентификации и аутентификации являются следующие**:

идентификация и аутентификация с помощью имени и пароля;

идентификация и аутентификация с помощью внешних носителей ключевой информации;

идентификация и аутентификация с помощью биометрических характеристик пользователей.

С точки зрения безопасности каждый из перечисленных типов способствует решению своих специфических задач, поэтому процессы и протоколы аутентификации активно используются на практике.

Основными атаками на протоколы аутентификации являются:

маскировка – пользователь пытается выдать себя за другого с целью получения полномочий и возможности действий от лица другого пользователя;

подмена стороны аутентификационного обмена – злоумышленник в ходе данной атаки участвует в процессе аутентификационного обмена между двумя сторонами с целью модификации проходящего через него трафика;

повторная передача – заключается в повторной передаче аутентификационных данных каким-либо пользователем;

принудительная задержка – злоумышленник перехватывает некоторую информацию и передает ее спустя некоторое время;

атака с выборкой текста – злоумышленник перехватывает аутентификационный трафик и пытается получить информацию о долговременных криптографических ключах.

Для предотвращения таких атак при построении протоколов аутентификации применяются следующие приемы:

использование механизмов типа «запрос-ответ», меток времени, случайных чисел, идентификаторов, электронных цифровых подписей;

привязка результата аутентификации к последующим действиям пользователей в рамках ИС. Примером подобного подхода может служить осуществление в процессе аутентификации обмена секретными сеансовыми ключами, которые используются при дальнейшем взаимодействии пользователей;

периодическое выполнение процедур аутентификации в рамках уже установленного сеанса связи и т. п.

Особое значение в контексте защиты информации от НСД имеет парольная политика для сотрудников, выполняющих функции пользователей ЕЦП. Так, для их доступа требуется использование имени пользователя (логина) и пароля. Имя пользователя должно быть уникальное в границах системы заведения учетных записей пользователей. Имя пользователя не должно явно указывать на уровень прав и привилегий.

При формировании пароля (ручном и автоматическом режиме) и настройке правил его применения необходимо учитывать следующие параметры:

минимальная длина пароля – не менее 8 символов;

максимальный срок использования пароля – не более 1 года для пользователей ИС;

максимальный срок использования пароля – не более 3 месяцев для пользователей СВТ, учетных записей администраторов и учетных записей с расширенными правами доступа;

повторяемость пароля – последние использовавшиеся 4 пароля не должны совпадать;

обязательная принудительная смена начального значения пароля при первом входе субъекта доступа в учетную запись или прикладное ПО;

блокирование доступа к ИС при неверно введенных данных в процессе повторного установления подлинности.

Сложность паролей должна удовлетворять следующим минимальным требованиям:

пароль не должен содержать имя учетной записи или какую–либо его часть;

пароль не основан на персональных данных (имена, телефонные номера, даты рождения и другие);

пароль не содержит последовательности одинаковых цифр или букв;

пароль должен состоять не менее чем из 8 символов;

в пароле должны присутствовать символы 3 категорий из числа следующих 4:

прописные буквы английского алфавита от A до Z;

строчные буквы английского алфавита от a до z;

десятичные цифры (от 0 до 9);

неалфавитные символы (например: !,$,#, %).

При использовании паролей сотрудники обязаны:

хранить атрибуты учетных записей в тайне и не передавать, и не сообщать третьим лицам;

изменять пароли при любом признаке возможной компрометации пароля;

выбирать качественные пароли, удовлетворяющие требованиям, которые возможно запомнить;

избегать многократного использования или кругового повторения старых паролей;

не включать пароли в какие–либо процессы автоматизированного входа, например, сохранение с помощью макроса или функциональной клавиши;

не делиться индивидуальными паролями;

не использовать один и тот же пароль для служебных и неслужебных целей.

При первой регистрации начальное (техническое) значение его пароля должно быть заменено. Для передачи начального (технического) значения пароля администратор ИБ обязан использовать средства, исключающие возможность нарушения конфиденциальности пароля.

1.3. Разграничение доступа к объектам ОС

Разграничение доступа к объектам ОС *– это порядок использования ИС, при котором субъекты получают доступ к объектам системы в строгом соответствии с установленными правилами.*

Основными понятиями процесса разграничения доступа к объектам ОС являются: объект доступа, метод доступа к объекту и субъект доступа.

Объектом доступа (или просто объектом) называют любой элемент ОС, доступ к которому пользователей и других субъектов доступа может быть произвольно ограничен. Возможность доступа к объектам ОС определяется не только архитектурой ОС, но и текущей политикой безопасности. Под объектами доступа понимают, как ресурсы оборудования, так и программные ресурсы. В качестве примера ресурсов оборудования можно привести процессор, принтер, жесткие диски. Каждый объект имеет уникальное имя, отличающее его от других объектов в системе, и может быть доступен через хорошо определенные и значимые операции.

Методом доступа к объекту называется операция, определенная для объекта. Тип операции зависит от объектов. Например, процессор может только выполнять команды, сегменты памяти могут быть записаны и прочитаны, считыватель магнитных карт может только читать, а для файлов могут быть определены методы доступа «чтение», «запись» и «добавление» (дописывание информации в конец файла).

Субъектом доступа называют любую сущность, способную инициировать выполнение операций над объектами (обращаться к объектам по некоторым методам доступа). Обычно полагают, что множество субъектов доступа и множество объектов доступа не пересекаются.

Иногда к субъектам доступа относят процессы, выполняющиеся в системе. Однако логичнее считать субъектом доступа именно пользователя, от имени которого выполняется процесс. Естественно, под субъектом доступа подразумевают не физического пользователя, работающего с компьютером, а «логического», от имени которого выполняются процессы ОС.

Таким образом, объект доступа – это то, к чему осуществляется доступ, субъект доступа – это тот, кто осуществляет доступ, и метод доступа – это то, как осуществляется доступ.

Для объекта доступа может быть определен *владелец* – субъект, которому принадлежит данный объект и который несет ответственность за

конфиденциальность содержащейся в объекте информации, а также за целостность и доступность объекта.

Обычно владельцем объекта автоматически назначается субъект, создавший данный объект; в дальнейшем владелец объекта может быть изменен с использованием соответствующего метода доступа к объекту. На владельца, как правило, возлагается ответственность за корректное ограничение прав доступа к данному объекту других субъектов.

Правом доступа к объекту называют право на получение доступа к объекту по некоторому методу или группе методов. Например, если пользователь имеет возможность читать файл, говорят, что он имеет право на чтение этого файла. Говорят, что субъект имеет некоторую привилегию, если он имеет право на доступ по некоторому методу или группе методов ко всем объектам ОС, поддерживающим данный метод доступа.

Разграничением доступа субъектов к объектам является совокупность правил, определяющая для каждой тройки субъект–объект–метод, разрешен ли доступ данного субъекта к данному объекту по данному методу. При избирательном разграничении доступа возможность доступа определена однозначно для каждой тройки субъект–объект–метод, при полномочном разграничении доступа ситуация несколько сложнее.

Субъекта доступа называют суперпользователем, если он имеет возможность игнорировать правила разграничения доступа к объектам.

Правила разграничения доступа, действующие в ОС, устанавливаются администраторами системы при определении текущей политики безопасности. За соблюдением этих правил субъектами доступа следит монитор ссылок – часть подсистемы защиты ОС.

Правила разграничения доступа должны удовлетворять следующим требованиям:

правила разграничения доступа, принятые в ОС, должны соответствовать аналогичным правилам, принятым в организации, в которой установлена эта ОС. Иными словами, если согласно правилам организации, доступ пользователя к некоторой информации считается несанкционированным, этот доступ должен быть ему запрещен;

правила разграничения доступа не должны допускать разрушающие воздействия субъектов доступа на ОС, выражающиеся в несанкционированном изменении, удалении или другом воздействии на объекты, жизненно важные для нормальной работы ос

любой объект доступа должен иметь владельца. Недопустимо присутствие ничейных объектов – объектов, не имеющих владельца;

недопустимо присутствие недоступных объектов – объектов, к которым не может обратиться ни один субъект доступа ни по одному методу доступа;

недопустима утечка конфиденциальной информации.

Существуют две основные модели разграничения доступа:

избирательное (дискреционное) разграничение доступа;

полномочное (мандатное) разграничение доступа.

При *избирательном разграничении доступа* определенные операции над конкретным ресурсом запрещаются или разрешаются субъектам (группам субъектов).

Большинство ОС реализуют именно избирательное разграничение доступа.

Полномочное разграничение доступа заключается в том, что все объекты могут иметь уровни конфиденциальности, а все субъекты делятся на группы, образующие иерархию в соответствии с уровнем допуска к информации. Иногда эту модель называют моделью многоуровневой безопасности, предназначенной для хранения сведений ограниченного распространения.

Система правил избирательного разграничения доступа формулируется следующим образом:

для любого объекта ОС существует владелец;

владелец объекта может произвольно ограничивать доступ других субъектов к данному объекту;

для каждой тройки субъект–объект–метод возможность доступа определена однозначно;

существует хотя бы один привилегированный пользователь (администратор), имеющий возможность обратиться к любому объекту по любому методу доступа. Этот привилегированный пользователь не может

игнорировать разграничение доступа к объектам. Например, в ОС типа Windows администратор для обращения к чужому объекту (принадлежащему другому субъекту) должен вначале объявить себя владельцем этого объекта, используя привилегию администратора объявлять себя владельцем любого объекта, затем дать себе необходимые права, и только после этого администратор может обратиться к объекту. Последнее требование введено для реализации механизма удаления потенциально недоступных объектов.

При создании объекта его владельцем назначается субъект, создавший данный объект. В дальнейшем субъект, обладающий необходимыми правами, может назначить объекту нового владельца.

При этом субъект, изменяющий владельца объекта, может назначить новым владельцем объекта только себя. Такое ограничение вводится для того, чтобы владелец объекта не мог отдать владение объектом другому субъекту и тем самым снять с себя ответственность за некорректные действия с объектом.

Для определения прав доступа субъектов к объектам при избирательном разграничении доступа используются такие понятия, как *матрица доступа* и *домен безопасности*.

С концептуальной точки зрения текущее состояние прав доступа при избирательном разграничении доступа описывается *матрицей*, в строках которой перечислены субъекты доступа, в столбцах – объекты доступа, а в ячейках – операции, которые субъект может выполнить над объектом.

Домен безопасности определяет набор объектов и типов операций, которые могут производиться над каждым объектом ОС. Иными словами, это набор ресурсов, доступных субъекту. В рамках ОС любой процесс имеет домен, который является набором системных ресурсов, доступных процессу для выполнения им своих задач. Этими ресурсами могут быть сегменты памяти, пространство на жестком диске, службы ОС и другие процессы. В сетевой среде, домен является набором доступных физических и логических ресурсов, которыми могут быть маршрутизаторы, файловые серверы, службы FTP, веб-серверы и т.д.

Термин *домен безопасности* основывается на определении домена, добавляя к нему факт, что ресурсы в рамках этой логической структуры

(домена) работают с одной и той же политикой безопасности и управляются одной группой. Таким образом, администратор может поместить СВТ, учетные записи и сетевые ресурсы сотрудников отдела кадров организации в Домен 1, а компьютеры, учетные записи и сетевые ресурсы руководства организации в Домен 2. Все эти элементы попадут в эти два контейнера, поскольку они (элементы) не только выполняют однотипные задачи, но также, что более важно, имеют один и тот же уровень доверия. Общий уровень доверия позволяет управлять этими элементами одной (отдельной) политикой безопасности.

Связь конкретных субъектов, функционирующих в ОС, может быть организована следующим образом:

каждый пользователь может быть доменом. В этом случае набор объектов, к которым может быть организован доступ, зависит от идентификации пользователя;

каждый процесс может быть доменом. В этом случае набор доступных объектов определяется идентификацией процесса;

каждая процедура может быть доменом. В этом случае набор доступных объектов соответствует локальным переменным, определенным внутри процедуры. Заметим, что, когда процедура выполнена, происходит смена домена.

1.4. Политики безопасности ОС

Безопасность ОС основана на определенных правилах, регулирующих различные аспекты ее функционирования. Совокупность этих правил составляют единую политику безопасности.

В Windows 2000 и более поздних NT-образных ОС политика безопасности представляет собой две группы правил:

локальная политика безопасности, применяемая только к локальному компьютеру или пользователям (группе локальных пользователей). При этом, локальная политика является частью групповой политики безопасности;

локальная групповая политика безопасности, применяется в сетях, в которых присутствует контроллер домена – сервер, распространяющий

политики на группу СВТ в сети. Локальная групповая политика предоставляет сетевым администраторам возможность назначать определенные параметры рабочей среды для групп пользователей или компьютеров. Эти настройки применяются, когда пользователь из группы входит в систему на сетевом компьютере, или всякий раз, когда запускается СВТ в группе.

Локальные и групповые политики безопасности позволяют управлять различными штатными средствами системы:

политики для настройки встроенного брандмауэра Windows;

политики для управления электропитанием;

политики для настройки панели управления, панели задач и др.

политики для настройки антивирусной защиты;

политики для управления подключаемых устройств;

политики для настройки штатных средств шифрования

политики для настройки штатного браузера;

политики для настройки беспроводных сетей и др.

Для настройки параметров локальной групповой политики безопасности в операционной системе MS Windows 10 используется оснастка[2] «Редактор локальной групповой политики», запускаемая командой *gpedit.msc* в диалоговом окне «Выполнить» (Win+R). Данная оснастка служит для просмотра и редактирования объектов групповой политики (GPO), в которых хранятся параметры локальных политик безопасности для СВТ и пользователей. Она позволяет изменять политики, распространяющиеся как на компьютеры, так и на пользователей (учетные записи).

В панели пространства имен оснастки «Редактор локальной групповой политики» представлено два узла: *Конфигурация компьютера* и *Конфигурация пользователя* (рис. 1).

[2]Оснастка в Windows – программа, позволяющая настроить разные параметры операционной системы.

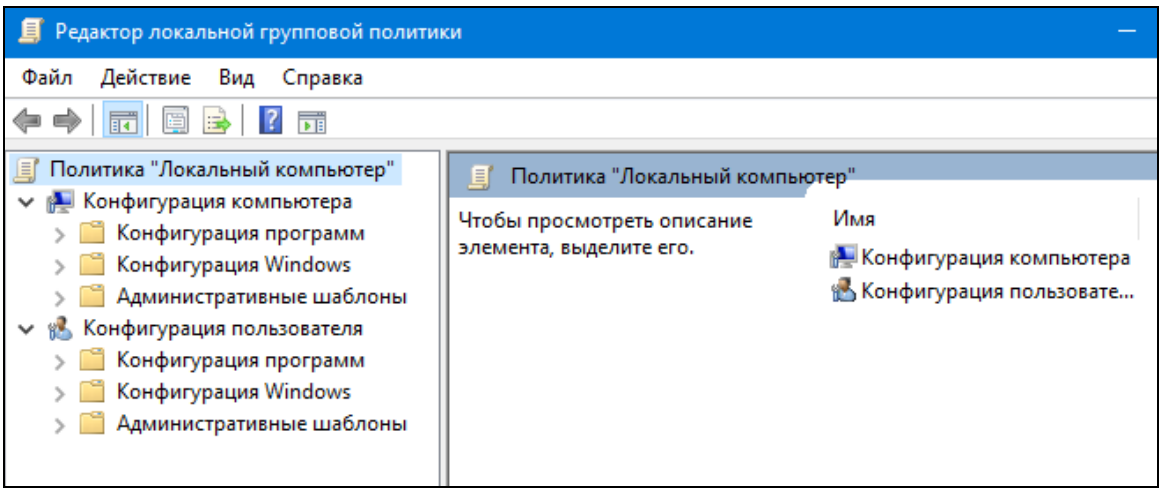


Рис. 1. Редактор локальной групповой политики

Узел *Конфигурация компьютера* содержит общесистемные настройки, определяющие работу СВТ. Эти политики регулируют функционирование операционной системы, определяют права пользователей в системе, работу системных служб и средств безопасности и т. д.

Узел *Конфигурация пользователя* содержит пользовательские настройки, определяющие работу пользователей СВТ (вид рабочего стола, параметры выполняющихся приложений, средств обеспечения безопасности и пользовательских сценариев входа и выхода и пр.).

В вышеприведенных узлах находятся по три дочерних узла (*конфигурация программ*, *конфигурация Windows*, *административные шаблоны)*, при помощи которых настраиваются все параметры локальных объектов групповых политик.

Для настройки параметров *локальной политики безопасности* используется команда *secpol.msc*, которая ограничивает настройку объектов локальной политики следующими параметрами и политиками (рис. 3):

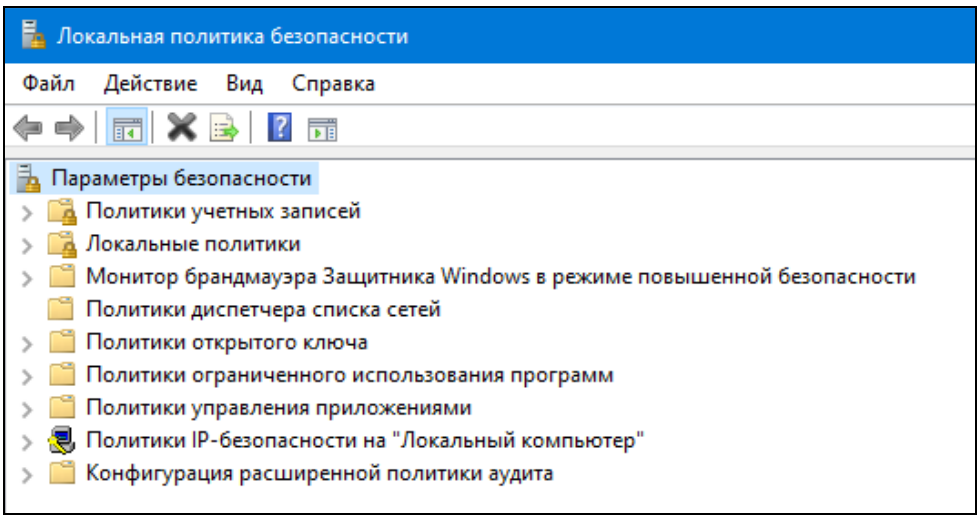


Рис. 3. Локальные политики безопасности Windows

Политики учетных записей. Определяют работу с паролями, а также условия блокировки учетных записей. Правила паролей задают требования, предъявляемые к паролям пользователей системы. Условия блокировки учетных записей предполагают установку времени до сброса счетчика блокировки, пороговое значение блокировки (количество ошибок ввода пароля при входе в систему) и продолжительность блокировки профиля пользователя.

Локальные политики. Включают сразу несколько групп параметров, разделенных по директориям: правила аудита событий, назначения привилегий пользователям и группам, а также раздел «Параметры безопасности», насчитывающий более тридцати параметров. Последние условно можно разделить на группы: аудиты, интерактивный вход в систему, контроль учетных записей, сетевой доступ, устройства и сетевая безопасность.

Брандмауэр Windows в режиме повышенной безопасности. Определяют правила блокировки либо разрешения для программ, портов или предопределенных соединений. В этом же разделе происходит определение типа безопасности подключения – изоляция, сервер-сервер, туннель или освобождение от проверки подлинности.

Политики диспетчера списков сетей. Параметры безопасности, которые можно использовать для настройки различных аспектов того, как сети перечислены и отображаются на одном устройстве или на нескольких устройствах

Политики открытого ключа. Позволяют настроить, в частности, правила использования файловой системы с шифрованием EFS (Encrypted File System).

Политики ограниченного использования программ. Основанная на групповых политиках функция, которая выявляет программы, работающие на компьютерах в домене (сети), и управляет возможностью выполнения этих программ.

Политики управления приложениями. Определяет настройки инструмента «AppLocker», который включает в себя множество самых разнообразных функций и настроек, позволяющих регулировать работу с программами. Например, он позволяет создать правило, ограничивающее запуск всех приложений, кроме указанных, либо установить ограничение на изменение файлов программами, задав отдельные аргументы и исключения.

Политики безопасности IP на локальном компьютере. Определяют возможности самостоятельной настройки неограниченного количества правил безопасности (методы шифрования, ограничения на передачу и прием трафика, фильтрация по IP-адресам, разрешение или запрет на подключение к сети и пр.)

Настройка политики расширенной проверки. Включают правила аудита событий, назначения привилегий пользователям и группам и некоторые возможности защиты.

Таким образом, редакторы групповой и локальной политик безопасности Windows реализуют *стандартную локальную групповую политику* (первый уровень), позволяющую изменять системные и пользовательские настройки, которые будут применены для всех пользователей операционной системы, а также домена (сети).

Для того, чтобы настроить политики безопасности для *конкретных пользователей*, в операционной системе Windows предусмотрена дополнительная многоуровневая локальная групповая политика:

групповая политика для администраторов и не администраторов (второй уровень). Эта групповая политика содержит только конфигурационные параметры пользователя и применяется в зависимости от того, является ли используемая учетная запись пользователя членом локальной группы *Администраторы* или нет;

групповая политика для конкретного пользователя (третий уровень). Эта групповая политика содержит только конфигурационные параметры конкретного пользователя.

1.5. Регистрация и оперативное оповещение о событиях безопасности

1.5.1. Протоколирование и аудит: общие сведения

Механизмы регистрации предназначены для получения и накопления (с целью последующего анализа) информации о состоянии ресурсов ИС и о действиях субъектов, признанных администрацией ИС потенциально опасными для системы. Анализ собранной средствами регистрации информации позволяет выявить факты совершения нарушений, характер воздействий на систему, подсказать метод его расследования и способы поиска нарушителя и исправления ситуации.

Средства регистрации позволяют также получать исчерпывающую статистику по использованию тех или иных ресурсов, межсетевому трафику, использованию сервисов, попыткам НСД и т.п.

Одним из средств программной регистрации о событиях безопасности являются протоколирование и аудит.

Под *протоколированием* понимается сбор и накопление информации о событиях, происходящих в информационной системе. У каждого сервиса свой набор возможных событий, но в любом случае их можно разделить на внешние (вызванные действиями других сервисов), внутренние (вызванные действиями самого сервиса) и клиентские (вызванные действиями пользователей и администраторов).

Аудит *– это анализ накопленной информации, проводимый оперативно, в реальном времени или периодически (например, раз в день). Оперативный аудит с автоматическим реагированием на выявленные нештатные ситуации называется активным.*

Процедура протоколирования применительно к ОС заключается в регистрации в специальном журнале, называемом журналом событий, событий, которые могут представлять опасность для ОС. Необходимость включения в

защищенную ОС функций протоколирования обусловлена следующими обстоятельствами:

обнаружение попыток НСД является важнейшей задачей системы защиты, поскольку ее решение позволяет минимизировать ущерб от взлома и собирать информацию о методах вторжения;

подсистема защиты ОС может не отличить случайные ошибки пользователей от злонамеренных действий. Администратор, просматривая журнал событий, сможет установить, что произошло при вводе пользователем неправильного пароля – ошибка легального пользователя или атака злоумышленника. Если пользователь пытался угадать пароль 20–30 раз – это явная попытка подбора пароля;

администраторы ОС должны иметь возможность получать информацию не только о текущем состоянии системы, но и о том, как ОС функционировала в недавнем прошлом. Такую возможность обеспечивает журнал событий;

если администратор ОС обнаружил, что против системы проведена успешная атака, ему важно выяснить, когда была начата атака и каким образом она осуществлялась. Журнал событий может содержать всю необходимую информацию.

К числу событий, которые могут представлять опасность для ОС, обычно относят следующие:

вход или выход из системы;

операции с файлами (открыть, закрыть, переименовать, удалить);

обращение к удаленной системе;

смена привилегий или иных атрибутов безопасности (режима доступа, уровня благонадежности пользователя и т. п.).

Протоколирование событий осуществляется в соответствии с политикой аудита. Политика аудита – это совокупность правил, определяющих то, какие события должны регистрироваться в журнале аудита. Для обеспечения надежной защиты ОС в журнале аудита должны обязательно регистрироваться следующие события:

попытки входа/выхода пользователей из системы;

попытки изменения списка пользователей;

попытки изменения политики безопасности, в том числе и политики аудита.

Политика аудита должна оперативно реагировать на изменения в конфигурации ОС, в характере хранимой и обрабатываемой информации, а особенно на выявленные попытки атаки ОС.

ОС Windows ведет аудит событий по 9 категориям:

событий входа в систему;

управления учетными записями;

доступа к службе каталогов;

входа в систему;

доступа к объектам;

изменения политики;

использования привилегий;

отслеживания процессов;

системных событий.

Рассмотрим более подробно, какие события отслеживает каждая из категорий.

Аудит событий входа в систему. Аудит попыток пользователя войти в систему с другого компьютера или выйти из нее, при условии, что этот компьютер используется для проверки подлинности учетной записи.

Аудит управления учетными записями. Аудит событий, связанных с управлением учетными записями на компьютере: создание, изменение или удаление учетной записи пользователя или группы; переименование, отключение или включение учетной записи пользователя; задание или изменение пароля.

Аудит доступа к службе каталогов. Аудит событий доступа пользователя к объекту каталога Active Directory, для которого задана собственная системная таблица управления доступом.

Аудит входа в систему. Аудит попыток пользователя войти в систему с компьютера или выйти из нее.

Аудит доступа к объектам. Аудит событий доступа пользователя к объекту – например, к файлу, папке, разделу реестра, принтеру и т. п., – для которого задана собственная системная таблица управления доступом.

Аудит изменения политики. Аудит фактов изменения политик назначения прав пользователей, политик аудита или политик доверительных отношений.

Аудит использования привилегий. Аудит попыток пользователя воспользоваться предоставленным ему правом.

Аудит отслеживания процессов. Аудит таких событий, как активизация программы, завершение процесса, повторение дескрипторов и косвенный доступ к объекту.

Аудит системных событий. Аудит событий перезагрузки или отключения компьютера, а также событий, влияющих на системную безопасность или на журнал безопасности.

Решения об аудите конкретного типа событий безопасности принимаются в соответствии с политикой аудита локальной системы, называемой локальной политикой безопасности.

1.5.2. Особенности организации и порядка мониторинга, аудита событий ИБ и реагирования на инциденты (на примере ИБ ЕЦП):

Инциденты ИБ в ЕЦП по степени воздействия подразделяются на критичные и прочие инциденты ИБ.

К **критичным инцидентам ИБ** относятся инциденты ИБ, которые: воздействуют на наиболее важные (критичные) процессы;

требуют привлечения значительных материальных, технических и людских ресурсов для устранения последствий;

наносят ОВД существенный материальный вред.

Инциденты ИБ, отнесенные к критичным инцидентам ИБ, имеют наивысший приоритет.

Для сбора и хранения информации о событиях ИБ в ЕЦП используются журналы сбора событий. Сбор информации о событиях ИБ производится круглосуточно. События, связанные с ИБ (в том числе происходящие из–за

сбоев ОС, программных, аппаратных и (или) программно–аппаратных средств), сохраняются в журнале сбора событий с заданным уровнем детализации.

Централизованный сбор и хранение информации о событиях ИБ журналов сбора событий осуществляется в центрах управления ИБ в круглосуточном режиме *системой сбора и обработки данных событий ИБ (далее – SIEM–система) автоматизированным способом*.

Запись в журнале сбора событий SIEM–системы должна содержать по возможности полную информацию о событии ИБ.

Форма записи о событиях ИБ должна содержать в обязательном порядке следующие поля:

порядковый номер записи в журнале сбора событий;

идентификатор события ИБ;

дата и время события;

тип события ИБ (уведомление, ошибка, сбой и так далее);

источник события (IP–адрес, присвоенное сетевое имя и так далее);

описание источника (тип устройства, программного средства, месторасположение и так далее);

описание события ИБ.

Записи о событиях ИБ в журналах сбора событий должны в обязательном порядке содержать следующие сведения:

идентификаторы субъектов информационных отношений ЕЦП;

дата, время и подробности ключевых событий ИБ, например, вход и выход из системы;

идентификатор оборудования (при возможности);

записи об успешных и отклоненных попытках доступа к ЕЦП, данным и другим информационным ресурсам;

использование прав доступа;

использование системных утилит и приложений;

файлы, к которым осуществлялся доступ, и тип доступа;

сетевые адреса и протоколы (для средств межсетевого экранирования).

Для выполнения мониторинга (просмотра, анализа) событий ИБ в журналах сбора событий должна быть обеспечена возможность фильтрации

событий (записей) по типу событий, учетной записи, дате, типу объекта. Также должна обеспечиваться сортировка по любому атрибуту события.

Организационно–технические мероприятия, реализуемые средством сбора и аудита событий ИБ, направлены на сбор и сохранение сообщений о происходящих событиях ИБ с целью выявления угроз и инцидентов ИБ, а также их локализации, расследования и недопущения в будущем.

Средства сбора и аудита событий ИБ должны применяться на всех уровнях защиты и протоколировать следующие события ИБ:

события антивирусного ПО;

системные события ОС, связанные с ИБ;

действия пользователей и администраторов;

события, связанные с функционированием приложений;

попытки доступа к информационным ресурсам и активам ЕЦП;

изменение конфигурации ЕЦП;

использование административных привилегий;

события, регистрируемые средствами защиты информации и прикладным ПО;

активация и деактивация средств защиты информации.

Время хранения событий ИБ – не менее одного года. Должна быть предусмотрена выгрузка в архив с возможностью последующей опциональной очистки содержимого журналов сбора событий для записей старше одного года.

Средства ведения журналов сбора событий и информация, содержащаяся в них, должны быть защищены от НСД путем применения средств разграничения доступа. Записи журналов сбора событий должны быть защищены.

1.6. Настройка службы удостоверения приложений

В условиях, когда информационные ресурсы являются одним из наиболее ценных активов, крайне важно обеспечить доступ к ним только авторизованным пользователям. Имеющиеся в ОС Windows технологии управления доступом позволяют достаточно эффективно контролировать, к

чему пользователи могут получить доступ. Однако если пользователь запускает процесс, этот процесс имеет тот же уровень доступа к данным, что и у пользователя. В результате конфиденциальные либо критически важные сведения могут быть без труда удалены или переданы за пределы контролируемой зоны, если пользователь намеренно или случайно запускает вредоносное программное обеспечение.

Разнообразие форм ВПО значительно усложняет понимание пользователями того, что безопасно запускать, а что нет. Активированное ВПО может повредить содержимое жесткого диска, заполнить сеть запросами, вызвав атаку по типу «отказ в обслуживании» (DoS), передать конфиденциальные сведения в Интернет или нарушить безопасность компьютера.

Кроме того, разработчики ПО создают все больше приложений, которые могут быть установлены пользователями, не являющимися администраторами. Это может нарушить политику безопасности организации либо подразделения и позволит обойти традиционные решения по управлению приложениями, которые полагаются на невозможность установки приложений пользователями.

Устранить подобные уязвимости системы безопасности можно с помощью интегрированного сервиса AppLocker, который позволяет ограничить возможности запуска нежелательного (и потенциально злонамеренного) ПО пользователями или группами.

Сервис AppLocker подходит для организаций либо подразделений, которые используют групповую политику для управления своими компьютерами.

Ниже приведены примеры сценариев, при которых может использоваться AppLocker:

политика безопасности определяет использование только лицензионного программного обеспечения, поэтому нужно запретить пользователям запускать нелицензионное программное обеспечение, а также ограничить использование лицензионного программного обеспечения только авторизованными пользователями;

возможность того, что нежелательное программное обеспечение может появиться в среде, достаточно высока, поэтому необходимо снизить эту угрозу;

лицензия на приложение была отозвана или истек срок ее действия в вашей организации, поэтому вам необходимо предотвратить возможность ее использования всеми пользователями;

развернуто новое приложение или новая версия приложения, и необходимо запретить пользователям запускать старую версию;

отдельные программные средства не разрешены в организации, или только определенные пользователи имеют доступ к этим средствам;

отдельный пользователь или небольшие группы пользователей должны использовать определенное приложение, в доступе к которому отказано всем прочим пользователям;

некоторые компьютеры совместно используются пользователями, которые имеют различные потребности в плане программного обеспечения, а вам необходимо защитить определенные приложения;

помимо других мер необходимо управлять доступом к конфиденциальным данным через использование приложений.

Таким образом, сервис AppLocker поможет вам защитить цифровые активы вашей организации, снизить угрозы, связанные с использованием вредоносного ПО в вашей среде, и улучшить управление приложениями и поддержку политик управления приложениями.

Для обеспечения безопасности компьютерной системы целесообразно разделить полномочия администраторов компьютерной системы и аудиторов (пользователей с правами доступа к журналу аудита и изменения параметров аудита). Если этого не сделать, то возникнет ситуация, при которой установка параметров политики безопасности и проверка ее соблюдения сосредоточатся в одних руках, что будет противоречить принципу разграничения полномочий.

3.2. Методы и средства защиты информации в компьютерных системах.

Интенсивное развитие современных информационных технологий, все более широкое их использование в деятельности ОВД придает особую актуальность задаче постоянного совершенствования системы защиты информационных ресурсов ЕЦП. При этом очевидными становятся факторы, повышающие необходимость комплексного подхода к защите информации с учетом выявления и минимизации информационных КУИ. Рассмотрим основные методы и средства защиты информации, обрабатываемой в компьютерных системах, и составляющие основу комплексной системы защиты.

1. Криптографическое преобразование информации

1.1. Общие сведения о шифровании данных

Для обеспечения безопасности информации ограниченного распространения, обрабатываемой в ИС, необходимо поддерживать три основные функции:

защиту конфиденциальности передаваемых или хранимых в памяти данных;

подтверждение целостности и подлинности данных;

аутентификацию пользователей при входе в систему и установлении соединения.

Для реализации указанных функций используются криптографические технологии шифрования и ЭЦП, а также средства аутентификации, рассмотренные нами выше.

Конфиденциальность обеспечивается с помощью алгоритмов и методов симметричного и асимметричного шифрования, а также путем взаимной аутентификации абонентов на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт и т. п.

Целостность и подлинность передаваемых данных обычно достигается с помощью различных вариантов технологии ЭЦП, основанных на односторонних функциях и асимметричных методах шифрования.

Аутентификация разрешает устанавливать соединения только между легитимными пользователями и предотвращает доступ к средствам сети нежелательных лиц. Абонентам, доказавшим свою легитимность (аутентичность), предоставляются разрешенные виды сетевого обслуживания.

Основой большинства криптографических средств защиты информации является шифрование данных.

*Под **шифром** понимают совокупность процедур и правил криптографических преобразований, используемых для зашифрования и расшифрования информации по ключу шифрования.*

*Под **зашифрованием** информации понимается процесс преобразования открытой информации (исходный текст) в зашифрованный текст (шифртекст).*

*Процесс восстановления исходного текста по криптограмме с использованием ключа шифрования называют **расшифрованием (дешифрованием)**.*

***Ключ шифрования** является тем элементом, с помощью которого можно варьировать результат криптографического преобразования.* Данный элемент может принадлежать конкретному пользователю или группе пользователей и являться для них уникальным. Зашифрованная с использованием конкретного ключа информация может быть расшифрована только его владельцем (или владельцами).

Преобразование шифрования относительно преобразования расшифрования может быть:

симметричным,

асимметричным.

Соответственно различают два основных класса криптосистем: симметричные; асимметричные.

Охарактеризуем кратко основные типы криптоалгоритмов.

***Симметричное** шифрование использует один и тот же ключ как для зашифрования, так и для расшифрования информации.* Фактически оба ключа (зашифрования и расшифрования) могут и различаться, но если в каком-либо

криптоалгоритме их легко вычислить один из другого в обе стороны, такой алгоритм однозначно относится к симметричному шифрованию.

Симметричное шифрование подразделяется на два вида:

блочное,

поточное.

Хотя стоит сразу отметить, что в некоторых классификациях они не разделяются и считается, что поточное шифрование – это шифрование блоков единичной длины.

Блочное шифрование характеризуется тем, что информация предварительно разбивается на блоки фиксированной длины (например, 64 или 128 бит). При этом в различных криптоалгоритмах или даже в разных режимах работы одного и того же алгоритма блоки могут шифроваться как независимо друг от друга, так и «со сцеплением» – когда результат шифрования текущего блока данных зависит от значения предыдущего блока или от результата шифрования предыдущего блока.

Поточное шифрование применяется прежде всего тогда, когда информацию невозможно разбить на блоки. Например, есть некий поток данных, каждый символ которых требуется зашифровать и отправить, не дожидаясь остальных данных, достаточных для формирования блока. Алгоритмы поточного шифрования шифруют данные побитно или посимвольно.

***Асимметричное** шифрование характеризуется применением двух типов ключей: открытого – для зашифрования информации и секретного – для ее расшифрования.* Секретный и открытый ключи связаны между собой достаточно сложным соотношением. Главное в этом соотношении – легкость вычисления открытого ключа из секретного и невозможность (за ограниченное время при реальных ресурсах) вычисления секретного ключа из открытого при достаточно большой размерности операндов.

Рассмотренные виды шифрования обладают как преимуществами, так и недостатками относительно друг друга. Алгоритмы симметричного шифрования намного быстрее и требуют меньше вычислительной мощности, но их основным недостатком является распределение ключей. Поскольку один

и тот же ключ используется для шифрования и дешифрования информации, этот ключ должен быть передан всем, кому потребуется доступ, что естественно создает определенные риски.

В свою очередь, асимметричное шифрование решает проблему распределения ключей, используя открытые ключи для шифрования, а закрытые (приватные) – для дешифрования. Компромисс заключается в том, что асимметричные системы очень медленны по сравнению с симметричными и требуют гораздо большей вычислительной мощности из-за длины ключа.

Важным методом криптозащиты является ***хэширование*** – *контрольное преобразование информации, выполняемое как с использованием некоторого секретного ключа, так и без него.*

В основе хеширования лежит односторонний метод вычисления: обратное вычисление (расшифровку) произвести не представляется возможным, поскольку существующие стандарты хеширования не шифрует данные в прямом смысле этого слова, а вычисляет значение хеш-функции для заданного набора данных. Например, используя стандарт MD5 для текстовых данных длиной 1000 символов, пользователь получает дайджест из 32 цифр. Далее, для гипотетической расшифровки дайджеста нужно по имеющимся 32 символам определить какие именно 1000 символов были использованы, но это не реально даже с учётом того, что известно, что их было именно 1000, а не 3000 или 25. Поэтому взлом хеша не имеет никакого смысла.

Хэширование широко используется в различных методах защиты информации, в частности, для подтверждения целостности данных, если использование ЭЦП невозможно (например, из-за большой ресурсоемкости) или избыточно. Кроме того, данный метод применяется в схемах ЭЦП («подписывается» обычно хэш-значение данных, а не все данные целиком), а также в схемах аутентификации пользователей (при проверке, действительно ли пользователь является тем, за кого себя выдает).

Процесс хеширования широко применяется в программировании, веб-индустрии и ИБ. Указанные области применения охватывают следующие основные направления:

создание ЭЦП;

защищенное хранение паролей в базах данных ИС;

создание криптографических ключей;

проверка подлинности и целостности элементов файловой системы СВТ;

создание уникальных идентификаторов и др.

Так, в некоторых системах управления веб-сайтами (CMS) хеширование используется при организации хранения паролей учетных записей, номеров банковских кредитных карт и другой критически важной информации в базах данных (MySQL, MongoDB и др.). В случае взлома злоумышленниками таких баз к ним в руки попадёт только бесполезный набор символов.

Кроме того, хеш-код может использоваться и как контрольная сумма для сравнения файлов. Полное совпадение хеша означает идентичность сравниваемых файлов, то есть у двух различных файлов не может быть одинаковых хешей. Поэтому алгоритмы хеширования часто используется в различных файлообменных сетях, торрентах, архиваторах, при создании резервных копий, а также для организации защищенного документооборота.

Существуют различные алгоритмы хеширования (SHA-1, SHA-256, SHA-512, MD5 и др.), реализованные в виде как специальных программ, так и он-лайн сервисов.

Различают предварительное и линейное шифрование.

Предварительное шифрование подразумевает, что криптографическое преобразование информации будет произведено перед отправкой данных.

Линейное шифрование (шифрование в линию) – это вид шифрования, при котором процесс «искажения» информации идет параллельно с ее отправкой.

Для решения задач защиты информации ограниченного распространения, обрабатываемой в ИС, используются:

средства линейного шифрования, предназначенные для обеспечения конфиденциальности и контроля целостности информации при ее передаче посредством сетей электросвязи общего пользования;

средства ЭЦП, предназначенные для обеспечения подлинности и контроля целостности электронных документов; удостоверения информации, составляющей общую часть электронного документа; подписания электронной копии документа на бумажном носителе.

Для безопасной эксплуатации средств линейного шифрования обеспечиваются следующие меры:

доступ к средствам линейного шифрования должен быть ограничен путем размещения оборудования в запираемых помещениях;

средства линейного шифрования размещаются в серверных стойках или шкафах, оборудованных надежными механическими замками;

хранение носителей ключевой информации осуществляется в шкафах (ящиках, хранилищах) в условиях, исключающих бесконтрольный доступ к ним, а также их преднамеренное уничтожение.

Защита средств линейного шифрования и ключевой информации от НСД обеспечивается не только в режиме функционирования, но и при проведении ремонтных и регламентных работ.

Все действия со средствами линейного шифрования администраторы ИБ обязаны осуществлять только после осмотра устройства на целостность и отсутствие несанкционированных подключений к ним. Присутствие посторонних лиц при этом запрещено.

1.2. Электронная цифровая подпись: общие сведения, особенности использования

Электронная цифровая подпись (ЭЦП) используется для подтверждения целостности и авторства данных. Как и в случае асимметричного шифрования, в данном методе применяются двухключевые алгоритмы с таким же простым вычислением открытого ключа из секретного и практической невозможностью обратного вычисления. Однако назначение ключей ЭЦП совершенно иное. Секретный ключ применяется для вычисления ЭЦП, открытый ключ необходим для ее проверки. При соблюдении правил безопасного хранения секретного ключа никто, кроме его владельца, не в состоянии вычислить верную ЭЦП какого-либо электронного документа.

Функционально цифровая подпись аналогична обычной рукописной подписи и обладает ее основными достоинствами:

удостоверяет, что подписанный текст исходит от лица, поставившего подпись;

не дает самому этому лицу возможности отказаться от обязательств, связанных с подписанным текстом;

гарантирует целостность подписанного текста.

ЭЦП представляет собой относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом. ЭЦП основана на обратимости асимметричных шифров, а также на взаимосвязанности содержимого сообщения, самой подписи и пары ключей. Изменение хотя бы одного из этих элементов сделает невозможным подтверждение подлинности цифровой подписи. ЭЦП реализуется при помощи асимметричных алгоритмов шифрования и хэш-функций.

Технология применения системы ЭЦП предполагает наличие сети абонентов, посылающих друг другу подписанные электронные документы. Для каждого абонента генерируется пара ключей: секретный и открытый. Секретный ключ хранится абонентом в тайне и используется им для формирования ЭЦП. Открытый ключ известен всем другим пользователям и предназначен для проверки ЭЦП получателем подписанного электронного документа.

Система ЭЦП включает две основные процедуры:

процедуру формирования цифровой подписи;

процедуру проверки цифровой подписи.

В процедуре формирования подписи используется секретный ключ отправителя сообщения, в процедуре проверки подписи – открытый ключ отправителя.

Процедура формирования цифровой подписи. На подготовительном этапе этой процедуры абонент *A* - отправитель сообщения генерирует пару ключей: секретный ключ *kA* и открытый ключ *KA*. Открытый ключ *KA* вычисляется из парного ему секретного ключа *kA*. Открытый ключ *KA* рассылается остальным абонентам сети (или делается доступным, например, на разделяемом ресурсе) для использования при проверке подписи.

Для формирования цифровой подписи отправитель *A* прежде всего вычисляет значение хэш-функции *h(M)* подписываемого текста *M* (рис. 2).

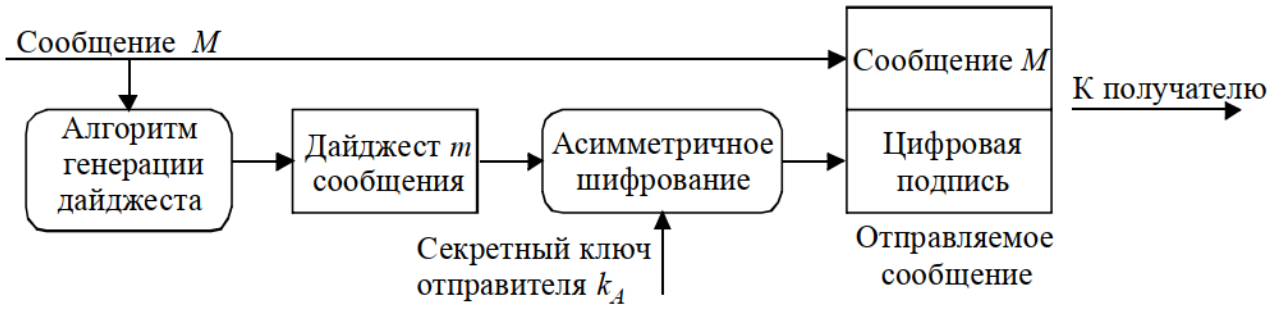


Рис. 2. Схема формирования электронной цифровой подписи

Хэш-функция служит для сжатия исходного подписываемого текста *M* в дайджест *m* – относительно короткое число, состоящее из фиксированного небольшого числа битов и характеризующее весь текст *M* в целом.

Далее отправитель *A* шифрует дайджест m своим секретным ключом *kA*. Получаемая при этом пара чисел представляет собой цифровую подпись для данного текста *M*. Сообщение *M* вместе с цифровой подписью отправляется в адрес получателя.

Процедура проверки цифровой подписи. Абоненты сети могут проверить цифровую подпись полученного сообщения *Mc* помощью открытого ключа отправителя *KA* этого сообщения (рис.3).

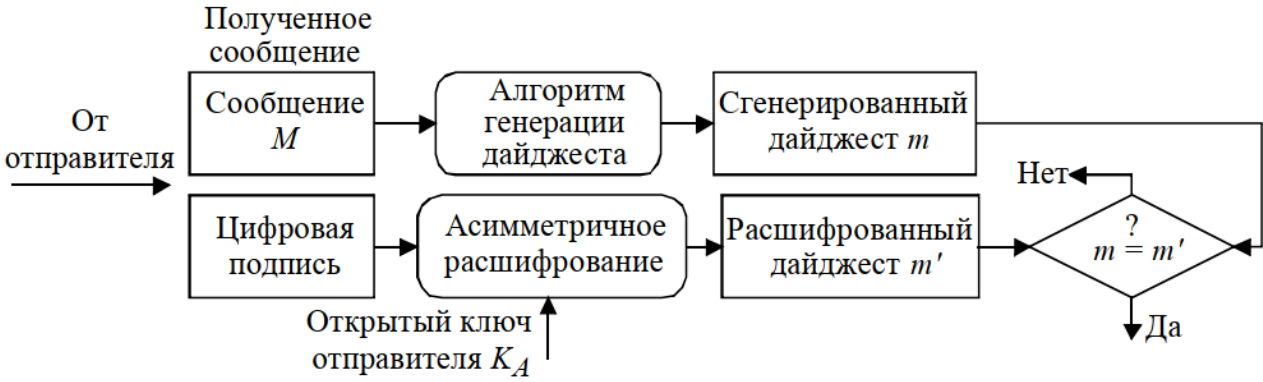


Рис. 3. Схема проверки электронной цифровой подписи

При проверке ЭЦП абонент *B* – получатель сообщения *M* расшифровывает принятый дайджест m открытым ключом *KA* отправителя *A*. Кроме того, получатель сам вычисляет с помощью хэш-функции *h(M)* дайджест *m'* принятого сообщения *M* и сравнивает его с расшифрованным. Если эти два дайджеста *m* и *m*' совпадают, то цифровая подпись является подлинной. В противном случае либо подпись подделана, либо изменено содержание сообщения.

Принципиальным моментом в системе ЭЦП является невозможность подделки ЭЦП пользователя без знания его секретного ключа подписывания. Поэтому необходимо защитить секретный ключ подписывания от НСД. Секретный ключ ЭЦП аналогично ключу симметричного шифрования рекомендуется хранить на персональном ключевом носителе в защищенном виде.

Таким образом, ЭЦП представляет собой уникальное число, зависящее от подписываемого документа и секретного ключа абонента. В качестве подписываемого документа может быть использован любой файл. Подписанный файл создается из неподписанного путем добавления в него одной или более электронных подписей.

Помещаемая в подписываемый файл (или в отдельный файл электронной подписи) структура ЭЦП обычно содержит дополнительную информацию, однозначно идентифицирующую автора подписанного документа. Эта информация добавляется к документу до вычисления ЭЦП, что обеспечивает и ее целостность. Каждая подпись содержит следующую информацию:

дату подписи;

срок окончания действия ключа данной подписи;

информацию о лице, подписавшем файл (Ф.И.О., должность, наименование организации);

идентификатор подписавшего (имя открытого ключа);

собственно цифровую подпись.

Важно отметить, что с точки зрения конечного пользователя процесс формирования и проверки цифровой подписи отличается от процесса

криптографического закрытия передаваемых данных следующими особенностями.

При формировании цифровой подписи используются закрытый ключ отправителя, тогда как при зашифровании используется открытый ключ получателя. При проверке цифровой подписи используется открытый ключ отправителя, а при расшифровании - закрытый ключ получателя.

Проверить сформированную подпись может любое лицо, так как ключ проверки подписи является открытым. При положительном результате проверки подписи делается заключение о подлинности и целостности полученного сообщения, т.е. о том, что это сообщение действительно отправлено тем или иным отправителем и не было модифицировано при передаче по сети.

1.3. Порядок применения ЭЦП субъектами ЕЦП

Для применения ЭЦП субъектами ЕЦП необходимы:

средство комплексной защиты информации для удостоверения записей ЭЦП;

МНИ с личным ключом потребителя (USB–токены, смарт–карты, SIM–карты из комплекта поставки).

Внутренний пользователь ЕЦП, получивший полномочия применять ЭЦП, может являться владельцем одного средства ЭЦП (при этом владельцем средства ЭЦП может быть только одно лицо).

Внутренние пользователи ЕЦП, получившие полномочия применять ЭЦП, регистрируются в соответствующем удостоверяющем центре с целью проверки данных о владельце личного ключа, дополнительных атрибутов в запросах на сертификат и формирования запросов в удостоверяющем центре.

Перед подписанием ЭЦП электронных документов, при внесении и (или) изменении данных электронных документов, перед прохождением процедуры аутентификации осуществляется проверка подлинности сертификата открытого ключа субъекта информационных отношений ЕЦП на момент использования, подлинности цепочки сертификатов до корневого, включая проверку сроков действия сертификатов.

При проверке подлинности сертификатов открытых ключей формируется сообщение с подтверждением формирования ЭЦП или обоснованием невозможности формирования ЭЦП для следующих случаев:

срок действия сертификата истек;

сертификат временно приостановлен;

сертификат отозван.

Хранение МНИ с личным ключом потребителя осуществляется в шкафах (ящиках, хранилищах) индивидуального пользования в условиях, исключающих бесконтрольный доступ к ним, а также их преднамеренное уничтожение.

В случае компрометации криптографического ключа внутренний пользователь ЕЦП, получивший полномочия применять ЭЦП, обязан незамедлительно прекратить обмен электронными документами с использованием скомпрометированных криптографических ключей и уведомить администратора ИБ.

Администратор ИБ или аудитор ИБ формирует и направляет в удостоверяющий центр заявку на приостановление действия сертификата, в которой необходимо указать:

идентификационные параметры скомпрометированного криптографического ключа;

фамилию, имя, отчество субъекта информационных отношений, который владел скомпрометированным криптографическим ключом;

сведения об обстоятельствах компрометации криптографического ключа;

время и обстоятельства выявления факта компрометации криптографического ключа.

Администратор ИБ или аудитор ИБ также формирует и направляет заявку на приостановление действия сертификата при отсутствии необходимости дальнейшего использования средства ЭЦП.

Для уменьшения вероятности раскрытия криптографических ключей возможно использование ключа только в течение заданного периода времени. Перевыпуск ключа производится по истечении заданного периода времени, а

также по мере необходимости в соответствии с процедурами, установленными удостоверяющим центром.

Использование средств ЭЦП может быть возобновлено только после ввода в действие другого криптографического ключа взамен скомпрометированного.

Скомпрометированные ключи подлежат уничтожению. Уничтожение ключей и всех резервных копий ключевой информации выполняется в соответствии с процедурами, установленными удостоверяющим центром.

2. Организация использования доверенных внешних МНИ

Обработка защищаемой информации в рамках ЕЦП выполняется только на зарегистрированных МНИ или разрешенных в установленном порядке (далее – доверенные МНИ).

Перечень доверенных МНИ учитывается в электронном виде администраторами ИБ соответствующего уровня. Для возможности использования доверенных МНИ в ЕЦП сотрудники предоставляют для регистрации их администратору ИБ соответствующего уровня. Допускается ведение перечня с использованием программных средств защиты информации.

При регистрации МНИ учитываются:

идентификатор МНИ (S/N, VID/PID, собственный ID);

информация о владельце или ответственном пользователе съемного носителя информации (фамилия, инициалы);

дата регистрации МНИ.

Внутренним пользователям ЕЦП запрещается использовать доверенные МНИ в личных целях и передавать их третьим лицам.

При изменении владельца или ответственного пользователя необходимо удаление информации, хранимой на МНИ. Для снижения вероятности восстановления удаленной информации применяется метод многократной перезаписи случайными последовательностями.

Физическое уничтожение доверенных МНИ, используемых в ЕЦП, осуществляется в следующих случаях:

МНИ испорчен или выведен из строя;

при истечении срока хранения информации, содержащейся на однократно записываемом МНИ;

при выводе из эксплуатации МНИ.

Владелец или ответственный пользователь незамедлительно сообщает администратору ИБ о фактах утраты доверенного МНИ.

Ответственность за сохранность МНИ, а также за утечку защищаемой информации, записанной на данный носитель, несет владелец или ответственный пользователь.

3. Защита периметра ИС

Для защиты периметра ИС и ЛВС при осуществлении информационно-коммуникационного взаимодействия с другими ИС и внешними сетями, разграничения доступа между сегментами ЛВС, а также для защиты от проникновения и вмешательства нарушителей из внешних систем применяются средства межсетевого экранирования.

Межсетевое экранирование *представляет собой программное (программно-аппаратное) средство защиты информации, осуществляющее анализ и фильтрацию проходящих через него сетевых пакетов.*

В зависимости от установленных правил, МЭ пропускает или уничтожает пакеты, разрешая или запрещая таким образом сетевые соединения. МЭ является классическим средством защиты периметра ЛВС: он устанавливается на границе между внутренней (защищаемой) и внешней (потенциально опасной) сетями и контролирует соединения между узлами этих сетей.

Для противодействия несанкционированному межсетевому доступу МЭ должен располагаться между защищаемой сетью организации, являющейся внутренней, и потенциально враждебной внешней сетью (рис. 9). При этом все взаимодействия между этими сетями должны осуществляться только через МЭ. Организационно МЭ входит в состав защищаемой сети.

Фильтрация информационных потоков состоит в их выборочном пропускании через МЭ, возможно, с выполнением некоторых преобразований. Фильтрация осуществляется на основе набора предварительно загруженных в МЭ правил, соответствующих принятой политике безопасности. Поэтому МЭ

удобно представлять как последовательность фильтров, обрабатывающих информационный поток.

Каждый из фильтров МЭ предназначен для интерпретации отдельных правил фильтрации путем:

анализа информации по заданным в интерпретируемых правилах критериям, например по адресам получателя и отправителя или по типу приложения, для которого эта информация предназначена;

принятия на основе интерпретируемых правил одного из следующих решений:

не пропустить данные;

обработать данные от имени получателя и возвратить результат отправителю;

передать данные на следующий фильтр для продолжения анализа;

пропустить данные, игнорируя следующие фильтры.

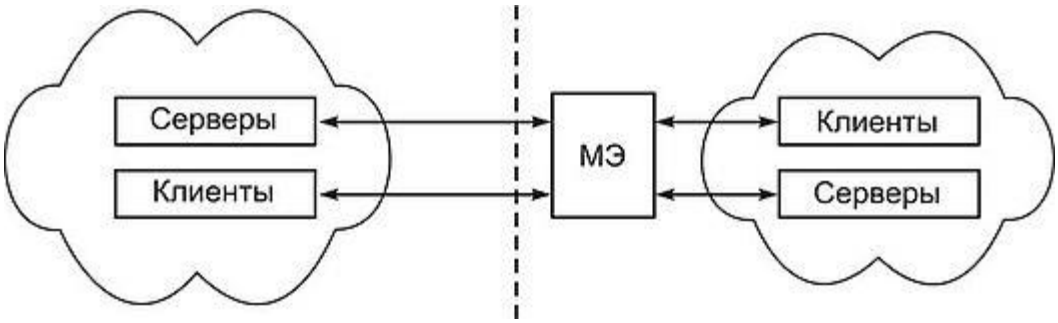


Рис. 9. Схема подключения межсетевого экрана МЭ

Правила фильтрации могут задавать и дополнительные действия, которые относятся к функциям посредничества, например, преобразование данных, регистрация событий и др. Соответственно правила фильтрации определяют перечень условий, по которым осуществляется:

разрешение или запрещение дальнейшей передачи данных;

выполнение дополнительных защитных функций.

В качестве критериев анализа информационного потока могут использоваться следующие параметры:

служебные поля пакетов сообщений, содержащие сетевые адреса, идентификаторы, адреса интерфейсов, номера портов и другие значимые данные;

непосредственное содержимое пакетов сообщений, проверяемое, например, на наличие ВПО;

внешние характеристики потока информации, например, временные, частотные характеристики, объем данных и т. д.

Настройка и конфигурирование средств МЭ ЕЦП осуществляются администраторами сети и администраторами ИБ.

Для обеспечения сетевой безопасности ЕЦП при внешних взаимодействиях должны использоваться средства МЭ с системами обнаружения и предотвращения вторжений (IPS и IDS), потокового антивируса которые обеспечивают:

фильтрацию входящего и (или) исходящего сетевого трафика на канальном, сетевом и прикладном уровнях;

управление потоками сетевого трафика в рамках информационного обмена в соответствии с настроенными правилами доступа;

ограничение открытых сетевых портов исключительно необходимыми;

сбор событий ИБ;

анализ событий ИБ.

Средства МЭ должны быть установлены на границах контролируемых зон ЕЦП.

Первоначальная настройка средств МЭ должна обеспечивать:

запрет на любое взаимодействие, кроме доступа администраторов сети и администраторов ИБ для дальнейшей настройки. Дальнейшая настройка должна осуществляться по принципу «запрещено все, что не разрешено»;

ограничение доступа для дальнейшей настройки по IP-адресам СВТ администратора сети и администратора ИБ;

настройку даты и времени (по возможности с привязкой к NTP серверу).

Применяемые средства МЭ должны иметь сертификаты соответствия, выданные в Национальной системе подтверждения соответствия Республики Беларусь.

Первоначальная настройка сетевого оборудования должна обеспечивать:

смену первоначальных логинов и паролей, установленных по умолчанию;

закрытие неиспользуемых протоколов доступа к администрированию;

ограничение по использованию протоколов удаленного доступа (SSH, HTTPs);

настройку даты и времени (при технической возможности с обязательной привязкой к NTP серверу);

ограничение доступа по IP–адресам;

логирование подключений и изменений конфигурации;

создание ACL–листов[3].

4. Выявление и нейтрализация действий ВПО, обнаружение атак (опасных действий нарушителей) и оперативное реагирование

Основными каналами проникновения ВПО являются:

инфицированные файлы со съемных МНИ;

инфицированное ПО, скрипты, апплеты и другие активные программные элементы, загруженные из общедоступных сетей связи и сохраненные на СВТ и серверы;

инфицированные удаленные СВТ и серверы при подключении к ЕЦП;

электронные письма, содержащие во вложенных файлах ВПО.

Обнаружение известных видов ВПО основано на ***сигнатурах****, т.е. характерных признаках, используемых для его обнаружения. Такой метод еще называется сигнатурным анализом.*

Принцип его работы заключается в том, что антивирусное ПО, просматривая файл или сетевой пакет, обращается к базе с известными вирусами, составленной разработчиками программы. В случае соответствия какого-либо участка кода просматриваемой программы известному коду (сигнатуре) вируса в базе, программа антивирус фиксирует факт обнаружения. Данный механизм обнаружения позволяет определять наличие вредоносного кода практически гарантированно и допускает минимальное количество ложных срабатываний.

[3] ACL (Access Control List) – список управления доступом, который определяет, кто или что может получать доступ к объекту (программе, процессу или файлу), и какие именно операции разрешено или запрещено выполнять субъекту (пользователю, группе пользователей).

Вместе с тем, сигнатурный анализ обладает и рядом существенных недостатков. Так он неспособен выявить новые вредоносные программы, полиморфные вирусы, которые способны к модификации собственного кода, а также даже незначительно изменённые версии ранее известного вируса.

Для выявления полиморфных и модифицированных вирусов в антивирусном ПО применяется механизм *эвристического сканирования*. Он служит для тех случаев, когда сигнатура из вирусной базы совпадает с кодом неизвестной программы не полностью, но содержит некоторые характерные признаки. В современных антивирусных ПО данная технология применяется крайне осторожно, так, чтобы не произошло серьезного повышения вероятности ложного срабатывания.

Для защиты от ВПО могут использоваться:

общие методы и средства защиты информации;

специализированное ПО;

профилактические мероприятия, позволяющие уменьшить вероятность заражения вирусами.

Общие средства защиты информации полезны не только для защиты от ВПО. Они используются также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователя. *Существуют две основные разновидности этих средств:*

средства копирования информации (применяются для создания копий файлов и системных областей дисков);

средства разграничения доступа (предотвращают несанкционированное использование информации, в частности обеспечивают защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей).

При заражении компьютера ВПО важно его обнаружить.

К внешним признакам проявления деятельности ВПО можно отнести следующие:

вывод на экран непредусмотренных сообщений или изображений;

подача непредусмотренных звуковых сигналов;

изменение даты и времени модификации файлов;

исчезновение файлов и каталогов или искажение их содержимого;

частые зависания и сбои в работе компьютера;

медленная работа компьютера;

невозможность загрузки ОС;

существенное уменьшение размера свободной оперативной памяти;

прекращение работы или неправильная работа ранее успешно функционировавших программ;

изменение размеров файлов;

неожиданное значительное увеличение количества файлов на диске.

Однако следует заметить, что перечисленные выше явления необязательно вызываются действиями ВПО, они могут быть следствием и других причин. Поэтому правильная диагностика состояния компьютера всегда затруднена и обычно требует привлечения специализированных программ.

Для обнаружения и защиты от ВПО разработано несколько видов специальных программ, которые позволяют обнаруживать и уничтожать компьютерные вирусы. Такие программы называются антивирусными. Практически все антивирусные программы обеспечивают автоматическое восстановление зараженных программ и загрузочных секторов. Антивирусные программы используют различные методы обнаружения вирусов.

К основным методам обнаружения ВПО и опасных действий нарушителей можно отнести следующие:

метод сравнения с эталоном;

эвристический анализ;

антивирусный мониторинг;

метод обнаружения изменений;

встраивание антивирусов в BIOS компьютера и др.

Метод сравнения с эталоном. Самый простой метод обнаружения заключается в том, что для поиска известных вирусов используются так называемые маски. Маской вируса является некоторая постоянная последовательность кода, специфичная для этого конкретного вируса. Антивирусная программа последовательно просматривает (сканирует)

проверяемые файлы в поиске масок известных вирусов. Антивирусные сканеры способны найти только уже известные вирусы, для которых определена маска.

Если вирус не содержит постоянной маски или длина этой маски недостаточно велика, то используются другие методы. Применение простых сканеров не защищает компьютер от проникновения новых вирусов. Для шифрующихся и полиморфных вирусов, способных полностью изменять свой код при заражении новой программы или загрузочного сектора, невозможно выделить маску, поэтому антивирусные сканеры их не обнаруживают.

Эвристический анализ. Для того чтобы размножаться, компьютерный вирус должен совершать какие-то конкретные действия: копирование в память, запись в секторы и т. д. Эвристический анализатор (который является частью антивирусного ядра) содержит список таких действий и проверяет программы и загрузочные секторы дисков, пытаясь обнаружить в них код, характерный для вирусов. Эвристический анализатор может обнаружить, например, что проверяемая программа устанавливает резидентный модуль в памяти или записывает данные в исполнимый файл программы. Обнаружив зараженный файл, анализатор обычно выводит сообщение на экране монитора и делает запись в собственном или системном журнале. В зависимости от настроек, антивирус может также направлять сообщение об обнаруженном вирусе администратору сети. Эвристический анализ позволяет обнаруживать неизвестные ранее вирусы. Практически все современные антивирусные программы реализуют собственные методы эвристического анализа.

Антивирусный мониторинг. Суть данного метода состоит в том, что в памяти компьютера постоянно находится антивирусная программа, осуществляющая мониторинг всех подозрительных действий, выполняемых другими программами. Антивирусный мониторинг позволяет проверять все запускаемые программы, создаваемые, открываемые и сохраняемые документы, файлы программ и документов, полученные через Интернет или скопированные на жесткий диск с дискеты либо компакт диска. Антивирусный монитор сообщит пользователю, если какая-либо программа попытается выполнить потенциально опасное действие. Примером такой программы

является Spider Guard, которая входит в комплект сканера Doctor Web и выполняет функции антивирусного монитора.

Метод обнаружения изменений. При реализации этого метода антивирусные программы, называемые ревизорами диска, запоминают предварительно характеристики всех областей диска, которые могут подвергнуться нападению, а затем периодически проверяют их. Заражая компьютер, вирус изменяет содержимое жесткого диска: например, дописывает свой код в файл программы или документа, добавляет вызов программы-вируса в файл AUTOEXEC.BAT, изменяет загрузочный сектор, создает файл-спутник. При сопоставлении значений характеристик областей диска антивирусная программа может обнаружить изменения, сделанные как известным, так и неизвестным вирусом.

Встраивание антивирусов в BIOS компьютера. В системные платы компьютеров встраивают простейшие средства защиты от вирусов. Эти средства позволяют контролировать все обращения к главной загрузочной записи жестких дисков, а также к загрузочным секторам МНИ. Если какая-либо программа пытается изменить содержимое загрузочных секторов, срабатывает защита, и пользователь получает соответствующее предупреждение. Однако эта защита не очень надежна. Известны вирусы, которые пытаются отключить антивирусный контроль BIOS, изменяя некоторые ячейки в энергонезависимой памяти (CMOS-памяти) компьютера.

В соответствии с ведомственными требованиями **антивирусная защита активов ЕЦП от ВПО реализуется**:

программными средствами защиты информации с централизованным управлением на республиканском, областном и районном уровнях;

потоковым антивирусом межсетевых экранов на республиканском и областном уровнях.

В целях минимизация рисков ИБ, связанных с утратой целостности, доступности и конфиденциальности информации, нарушением функционирования активов ЕЦП в результате воздействия ВПО антивирусная защита направлена на решение следующих задач:

обнаружение ВПО на активах ЕЦП (СВТ, виртуальные машины и серверы ЕЦП, прикладное ПО, файлы) путем постоянного мониторинга и периодического сканирования всех ресурсов ЕЦП;

контроль всех возможных каналов распространения ВПО;

автоматическое реагирование на заражение ВПО, включающее в себя оповещение, обезвреживание ВПО, предотвращение негативных последствий воздействия ВПО (очистка системы от ВПО);

непрерывный (в режиме реального времени) антивирусный мониторинг и периодическое (по требованию) антивирусное сканирование активов ЕЦП;

фиксация событий ИБ и отчетов о состоянии активов.

Обновление баз данных сигнатур ВПО и обновление модулей системы антивирусной защиты осуществляется на регулярной основе:

обновление сигнатур ВПО на сервере системы антивирусной защиты осуществляется администратором ИБ не реже одного раза в неделю;

автоматическое обновление выполняется централизованно с сервера системы антивирусной защиты или другой СВТ, ретранслирующей обновления;

ручное обновление баз данных сигнатур ВПО выполняет администратор ИБ со съемных носителей информации не реже одного раза в две недели.

Порядок действий при обнаружении ВПО состоит в следующем. При отображении на экране сообщения о том, что средством антивирусной защиты обезврежено ВПО, пользователи и администраторы продолжают работать в штатном режиме.

При подозрении в вирусном заражении пользователи и администраторы обязаны:

отключить СВТ от ведомственной сети передачи данных, а при необходимости – и от сети электропитания;

по согласованию с администратором ИБ или аудитором ИБ, принять меры по локализации и удалению ВПО с использованием системы антивирусной защиты.

Администратор ИБ обязан:

выполнить мероприятия по ликвидации заражения ПО;

провести анализ инцидента и причин, приведших к проникновению и воздействию ВПО на активы ЕЦП с учетом положений регламента мониторинга, аудита событий ИБ и реагирования на инциденты ИБ.

К мероприятиям по ликвидации последствий воздействия ВПО относятся:

анализ признаков проявления ВПО;

оценка полноты и корректности выполнения первоочередных действий по предотвращению распространения ВПО;

обновление баз данных сигнатур системы антивирусной защиты;

блокировка источника ВПО (IP–адрес и другие);

блокировка запуска ВПО по хэш–значению;

переустановка ОС или восстановление из резервной копии (при необходимости);

копирование с инфицированного СВТ критически важной информации с использованием системы антивирусной защиты;

анализ журналов сбора событий системы антивирусной защиты, ОС, прикладного ПО, активного сетевого оборудования;

обезвреживание и (или) удаление ВПО, восстановление поврежденных данных с последующей оценкой целостности восстановленных данных. При невозможности обезвреживания и (или) удаления ВПО, восстановления поврежденных данных выполняется форматирование носителя информации.

Своевременное обнаружение зараженных вирусами файлов и дисков, полное уничтожение обнаруженных вирусов на отдельно взятом СВТ позволяют избежать распространения вирусной эпидемии в сети. При этом следует учитывать, что абсолютно надежных антивирусных программ, гарантирующих обнаружение и уничтожение любого вируса, не существует. Важным методом борьбы с ВПО является своевременная профилактика.

4. Применение виртуальных частных сетей (VPN)

При подключении корпоративной ЛВС к сети Интернет возникают угрозы безопасности двух типов:

НСД к внутренним ресурсам корпоративной ЛВС;

НСД к корпоративным данным в процессе их передачи по открытой сети.

Обеспечение безопасности информационного взаимодействия ЛВС и отдельных СВТ через открытые сети, в частности через сеть «Интернет», возможно путем эффективного решения следующих задач:

защита подключенных к открытым каналам связи ЛВС и отдельных СВТ от несанкционированных действий со стороны внешней среды;

защита информации в процессе ее передачи по открытым каналам связи.

Для защиты ЛВС и отдельных СВТ от несанкционированных действий со стороны внешней среды обычно используют межсетевые экраны, которые располагаются на стыке между локальной и открытой сетью.

Защита информации в процессе ее передачи по открытым каналам основана на использовании виртуальных защищенных сетей VPN. ***Виртуальной защищенной сетью VPN (Virtual Private Network)*** *называют объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную сеть, обеспечивающую безопасность циркулирующих данных.*

Виртуальная защищенная сеть VPN формируется путем построения виртуальных защищенных каналов связи, создаваемых на базе открытых каналов связи общедоступной сети. Эти виртуальные защищенные каналы связи называются туннелями VPN. Сеть VPN позволяет с помощью туннелей VPN соединить территориально удаленные подразделения организации, удаленных пользователей и безопасно передавать информацию через Интернет.

Туннель VPN представляет собой сетевое соединение, реализованное через открытую сеть, по которому передаются криптографически защищенные пакеты сообщений виртуальной сети.

Защита информации в процессе ее передачи по туннелю VPN основана на выполнении следующих функций:

аутентификация взаимодействующих сторон;

криптографическое закрытие (шифрование) передаваемых данных;

проверка подлинности и целостности доставляемой информации.

При реализации этих функций используются криптографические методы защиты информации.

Эффективность такой защиты обеспечивается за счет совместного использования симметричных и асимметричных криптографических систем. Туннель VPN, формируемый устройствами VPN, обладает свойствами защищенной выделенной линии, причем эта защищенная выделенная линия развертывается в рамках общедоступной сети, например Интернета. Устройства VPN могут играть в виртуальных частных сетях роль VPN-клиента, VPN-сервера или шлюза безопасности VPN.

VPN-клиент *представляет собой программный или программно-аппаратный комплекс, выполняемый обычно на базе персонального компьютера.*

Его сетевое программное обеспечение модифицируется для выполнения шифрования и аутентификации трафика, которым это устройство обменивается с другими VPN-клиентами, VPN-серверами или шлюзами безопасности VPN. Обычно реализация VPN-клиента представляет собой программное решение, дополняющее стандартную ОС – Windows или Unix.

VPN-сервер *представляет собой программный или программно-аппаратный комплекс, устанавливаемый на компьютере, выполняющем функции сервера.*

VPN-сервер обеспечивает защиту серверов от НСД из внешних сетей, а также организацию защищенных соединений (ассоциаций) с отдельными СВТ и с СВТ из сегментов локальных сетей, защищенных соответствующими VPN-продуктами. VPN-сервер является функциональным аналогом продукта VPN-клиент для серверных платформ. Он отличается прежде всего расширенными ресурсами для поддержания множественных соединений с VPN-клиентами. VPN-сервер может поддерживать защищенные соединения с мобильными пользователями.

Шлюз безопасности VPN *– это сетевое устройство, подключаемое к двум сетям, которое выполняет функции шифрования и аутентификации для многочисленных хостов, расположенных за ним.*

Размещение шлюза безопасности VPN выполняется таким образом, чтобы через него проходил весь трафик, предназначенный для внутренней корпоративной сети. Сетевое соединение шлюза VPN прозрачно для

пользователей позади шлюза, оно представляется им выделенной линией, хотя на самом деле прокладывается через открытую сеть с коммутацией пакетов. Адрес шлюза безопасности VPN указывается как внешний адрес входящего туннелируемого пакета, а внутренний адрес пакета является адресом конкретного хоста позади шлюза. Шлюз безопасности VPN может быть реализован в виде отдельного программного решения, отдельного аппаратного устройства, а также в виде маршрутизатора или межсетевого экрана, дополненных функциями VPN.

Безопасность информационного обмена необходимо обеспечивать как в случае объединения локальных сетей, так и в случае доступа к ЛВС удаленных или мобильных пользователей. При проектировании VPN обычно рассматриваются две основные схемы:

виртуальный защищенный канал между локальными сетями (канал ЛВС – ЛВС);

виртуальный защищенный канал между узлом и локальной сетью (канал клиент – ЛВС) (рис.3).

Первая схема соединения позволяет создать постоянно доступные защищенные каналы между отдельными офисами. В этом случае шлюз безопасности служит интерфейсом между туннелем и ЛВС, и пользователи локальных сетей используют туннель для общения друг с другом.

Вторая схема защищенного канала VPN предназначена для установления соединений с удаленными или мобильными пользователями. Создание туннеля инициирует клиент (удаленный пользователь). Для связи со шлюзом, защищающим удаленную сеть, он запускает на своем компьютере специальное клиентское программное обеспечение. Этот вид VPN заменяет собой коммутируемые соединения и может использоваться наряду с традиционными методами удаленного доступа.

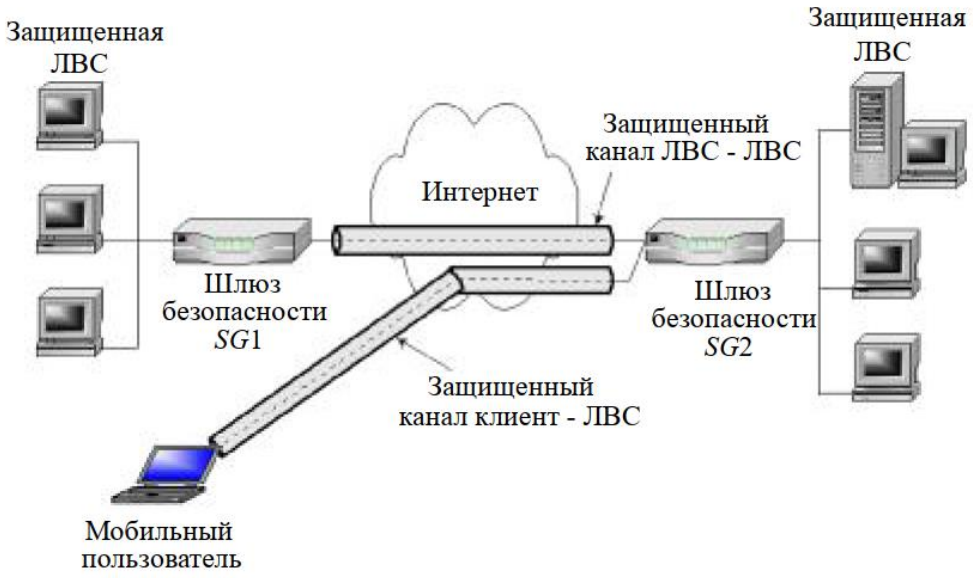


Рис. 3. Виртуальные защищенные каналы типа ЛВС - ЛВС и клиент - ЛВС

При построении защищенной виртуальной сети VPN первостепенное значение имеет задача обеспечения ИБ. Под безопасностью данных понимают их конфиденциальность, целостность и доступность.

Применительно к задачам VPN критерии безопасности данных могут быть определены следующим образом:

конфиденциальность – гарантия того, что в процессе передачи данных по защищенным каналам VPN эти данные могут быть известны только легальным отправителю и получателю;

целостность – гарантия сохранности передаваемых данных во время прохождения по защищенному каналу VPN;

доступность – гарантия того, что средства, выполняющие функции VPN, постоянно доступны легальным пользователям.

Конфиденциальность обеспечивается с помощью различных методов и алгоритмов симметричного и асимметричного шифрования.

Целостность передаваемых данных обычно достигается с помощью различных вариантов технологии электронной подписи, основанных на асимметричных методах шифрования и односторонних функциях.

Аутентификация осуществляется на основе многоразовых и одноразовых паролей, цифровых сертификатов, смарт-карт, протоколов строгой

аутентификации и обеспечивает установление VPN- соединения только между легальными пользователями и предотвращает доступ к средствам VPN нежелательных лиц.

Авторизация подразумевает предоставление абонентам, доказавшим свою легальность (аутентичность), разных видов обслуживания, в частности разных способов шифрования их трафика. Авторизация и управление доступом часто реализуются одними и теми же средствами.

Для обеспечения безопасности передаваемых данных в виртуальных защищенных сетях должны быть решены следующие основные задачи безопасности:

взаимная аутентификация абонентов при установлении соединения;

обеспечение конфиденциальности, целостности и аутентичности передаваемой информации;

авторизация и управление доступом.

Технологии обнаружения неконтролируемых источников угроз (HoneyPot и Deception)

Как уже ранее отмечалось, ИБ – это всесторонняя защищённость информации и поддерживающей её инфраструктуры от любых случайных или злонамеренных воздействий, результатом которых может явиться нанесение ущерба самой информации, ее владельцам или поддерживающей инфраструктуре. Задачи ИБ сводятся к минимизации ущерба, а также к прогнозированию и предотвращению таких воздействий. Это особенно актуально, поскольку в современных условиях вредоносные атаки становятся все более масштабными, а сами киберпреступники – лучше оснащёнными технологически.

В связи с этим набирают популярность решения класса ***HoneyPot***[4] ***и Deception***[5] – *программно-аппаратные средства, позволяющие в инфраструктуре компании создавать ложные сетевые объекты, которые принято называть ловушками (киберловушками, приманками и т. п.).*

[4] Переводится с английского как «горшочек с мёдом», интерпретируется как «приманка», «ловушка».

[5] Переводится с английского как «обман», интерпретируется как «создание ложных целей, расстановка ловушек».

Ключевой целью технологии HoneyPot является привлечение потенциальных злоумышленников и регистрация их деятельности в целях их раскрытия и обнаружения их намерений. Приманками HoneyPot может быть что угодно – от данных и информации до услуг или других ресурсов.

К наиболее распространенным видам приманок относятся:

различные учетные данные пользователей;

файлы различных подключений к удаленному рабочему столу;

записи в HOSTS файле;

сохраненные подключения к сетевым ресурсам и принтерам;

история команд в BASH и PowerShell;

история в браузерах и хранилище паролей в них;

сохраненные данные в браузерах;

сетевые подключения в SSH/FTP клиентах;

настройки популярных программ, хранящихся в реестре;

тестовые файлы с «забытыми» паролями;

менеджеры паролей вроде KeePass;

хранилища паролей типа MS Vault, оперативной памяти LSASS и кешей входа на рабочую станцию.

HoneyPot имитирует, будто в системах организации есть точки входа, не защищенные должным образом, тем самым привлекая потенциальных злоумышленников. Благодаря приманке, организация предотвращает атаки и может отследить и проанализировать действия хакеров. Это потенциально полезная стратегия, прежде всего для компаний, располагающих большим количеством конфиденциальных данных и являющихся привлекательной целью для злоумышленников.

Ловушка HoneyPot работает следующим образом:

устанавливается ряд серверов или систем, которые кажутся уязвимыми;

после установки ловушки, целью становится привлечение атакующих;

действия хакера, попавшего в «ловушку», находятся под контролем.

Таким образом, приманка HoneyPot – это сетевой объект, единственная цель которого – привлекать злоумышленника и быть атакованным. HoneyPot не несет иной ценности в сети, в которой установлен; с ним не ведется никаких

легитимных сетевых взаимодействий. Когда HoneyPot атакуют, он фиксирует это и сохраняет все действия атакующего. В дальнейшем эти данные помогают анализировать путь злоумышленника.

Однако сама по себе технология HoneyPot имеет ряд недостатков:

нужно отдельно настраивать каждый ложный сервер;

ловушки HoneyPot не взаимодействуют между собой и с элементами настоящей инфраструктуры.;

ловушки HoneyPot, как правило, не объединены в централизованную систему.

В настоящее время на смену этой технологии постепенно приходит другая, более усовершенствованная, – Deception.

Технология Deception относится к решениям класса Intrusion Detection System (IDS) – системам обнаружения вторжений. Основная цель такой системы – выявлять попытки нежелательного доступа к сети.

При внедрении технологии Deception информационная инфраструктура организации разделяется на две части. Первая – это реальная сеть компании, вторая – имитированная среда, состоящая из ловушек, расположенных на реальных физических устройствах. В рабочей инфраструктуре размещаются приманки и ловушки. Например, это могут быть ложные записи о подключении к сетевым дискам, учётные данные и другие сущности. Любое взаимодействие с ловушками означает вредоносную (хакерскую) активность. Соответственно, если злоумышленник попал в реальную инфраструктуру организации, добрался до рабочей станции или сервера, то он наткнётся на приманки и ловушки, которые передадут информацию о попытке атаки на компанию, и оператор получит подробности происходящего: IP-адрес и порт источника и цели, протокол взаимодействия, время срабатывания и т. д. Таким образом атакующий будет обнаружен и остановлен. В дальнейшем служба безопасности организации сможет проанализировать действия злоумышленников, узнать об их тактиках и целях. Эта информация позволит понять, что именно интересно злоумышленникам, и расставить акценты в защите данных. Создав обманную среду возможно уберечь ресурсы и приостановит атаку, отслеживая действия злоумашленника. Выгодно как можно убедительнее уверить злоумышленника

во взаимодействии с реальной инфраструктурой, чтобы обнаружить и противодействовать.

Технология Deception решает несколько основных задач, актуальных в рассматриваемом контексте:

создаёт поддельную инфраструктуру на базе существующей;

помогает обнаружить злоумышленника на начальном этапе проникновения в сеть при сканировании сетей или портов;

происходит обнаружение атакующего на этапе горизонтального перемещения – например, если злоумышленник скомпрометировал одно из автоматизированных рабочих мест и хочет переместиться на соседнее.

Технология Deception разработана с учётом анализа мышления и поведения злоумышленника и позволяет идентифицировать атаку на ранней стадии. Таким образом специалисты по ИБ получают значительное преимущество и выигрывают время в случае атаки. Также сотрудники собирают данные и анализируют действия нарушителя: как он смог проникнуть в инфраструктуру, что он для этого использовал, иными словами – проводят расследование.

Разные виды киберловушек используются для выявления разных угроз. Их свойства зависят от угрозы, для которой они созданы. У каждой ловушки своя роль в комплексной и эффективной стратегии кибербезопасности.

Почтовые ловушки, или ловушки для спама, помещают поддельный электронный адрес в хорошо спрятанное расположение, где его может найти только автоматический сборщик электронных адресов. Учитывая предназначение такого адреса, можно быть на 100% уверенным, что любое входящее по нему письмо – спам. Все письма, похожие на попавшие в ловушку, можно сразу блокировать, а IP-адрес отправителя заносить в черный список.

Поддельная база данных служит для наблюдения за уязвимостями ПО и обнаружения вредоносных атак, использующих ненадежную архитектуру систем или метод SQL-инъекции, эксплуатирующих SQL-службы или основанных на злоупотреблении привилегиями.

Ловушка для вредоносного ПО имитирует приложения, поощряя атаки ВПО. Атакующие программы подвергаются анализу для разработки защиты или устранения уязвимостей.

Анализируя входящий трафик ловушки, можно:

выяснить местонахождение киберпреступников;

оценить степень угрозы;

изучить методы злоумышленников;

узнать, какие данные или приложения их интересуют;

оценить эффективность используемых мер защиты от кибератак.

Средства управления событиями и инцидентами ИБ (SIEM-системы)

С растущим объемом информации, которая обрабатывается и передается между различными ИС, организации и отдельные пользователи все больше зависят от непрерывности и корректности выполнения данных процессов. Для реагирования на угрозы безопасности в ИС необходимо иметь инструменты, позволяющие анализировать в реальном времени происходящие события, число которых непрерывно растет. Одним из решений данной проблемы является использование SIEM-систем.

SIEM *– класс программных продуктов, предназначенных для сбора информации и дальнейшего ее анализа в целях выявления подозрительного поведения или потенциальных кибератак.*

SIEM *представляет собой объединение систем управления информационной безопасностью (SIM) и управления событиями безопасности (SEM) в единую систему управления безопасностью.*

Основополагающий принцип системы SIEM заключается в том, что данные о безопасности информационной системы собираются из разных источников, и результат их обработки предоставляется в едином интерфейсе, доступном для аналитиков безопасности, что облегчает изучение характерных особенностей, соответствующих инцидентам безопасности.

Сегмент SIM, в основном, отвечает за анализ исторических данных, стараясь улучшить долгосрочную эффективность системы и оптимизировать хранение исторических данных. Сегмент SEM, напротив, делает акцент на

выгрузке из имеющихся данных определенного объема информации, с помощью которого могут быть немедленно выявлены инциденты безопасности.

Одним из ключевых компонентов большинства SIEM-решений, представленных сегодня на рынке специализированного ПО, является подсистема сбора и анализа событий. Этот программный компонент консолидирует информацию из журналов событий, поступающую от различных устройств, конечных точек и приложений в сети; нормализует и анализирует корреляцию для выявления угроз безопасности; использует интеллектуальные механизмы для выявления нормального поведения, обнаружения аномалий, а также раскрытия угроз и удаления ложноположительных результатов.

Например, если сотрудник неудачно пытается войти в систему, предпринимая несколько попыток входа, а после сбрасывает пароль через почту – SIEM «прочитает» как обычный рабочий процесс. Но, если пароль водится десятки или сотню раз, а после наступает успех – система отправляет предупреждение о методе грубой силы.

Технология SIEM обеспечивает выполнению в реальном времени следующих основных задач:

сбор, обработка и анализ событий безопасности, поступающих в систему из множества источников;

обнаружение в режиме реального времени атак и нарушений критериев и политик безопасности;

оперативная оценка защищенности информационных, телекоммуникационных и других критически важных ресурсов;

анализ и управление рисками безопасности;

проведение расследований инцидентов;

принятие эффективных решений по защите информации;

формирование отчетных документов.

Для решения поставленных задач SIEM-системы первого поколения применяют нормализацию, фильтрацию, классификацию, агрегацию, корреляцию и приоритезацию событий, а также генерацию отчетов и предупреждений. В SIEM-системах нового поколения к их числу следует

добавить также анализ событий, инцидентов и их последствий, а также принятие решений и визуализацию.

Нормализация приводит форматы записей журналов, собранных из различных источников, к единому внутреннему формату, который затем будет использоваться для их хранения и последующей обработки.

Фильтрация событий безопасности заключается в удалении избыточных событий из поступающих в систему потоков.

Классификация позволяет для атрибутов событий безопасности определить их принадлежность определенным классам.

Агрегация предполагает управление журналами данных; данные собираются из различных источников: сетевые устройства и сервисы, датчики систем безопасности, серверы, базы данных, приложения; обеспечивается консолидация данных с целью поиска критических событий; объединяет события, схожие по определенным признакам.

Корреляция. осуществляет поиск общих атрибутов, связывание событий в значимые кластеры, выявляя взаимосвязи между разнородными событиями. Технология обеспечивает применение различных технических приемов для интеграции данных из различных источников для превращения исходных данных в значащую информацию.

Приоритезация определяет значимость и критичность событий безопасности на основании правил, определенных в системе.

Анализ событий, инцидентов и их последствий включает процедуры моделирования событий, атак и их последствий, анализа уязвимостей и защищенности системы, определения параметров нарушителей, оценки риска, прогнозирования событий и инцидентов.

Генерация отчетов и предупреждений означает формирование, передачу, отображение или печать результатов функционирования.

Визуализация предполагает представление в графическом виде данных, характеризующих результаты анализа событий безопасности и состояние защищаемой системы и ее элементов.

Таким образом, SIEM-системы являются важным звеном в архитектуре ИБ ИС, поскольку выполняет целый ряд ключевых задач: своевременное

обнаружение целенаправленных атак и непреднамеренных нарушений ИБ со стороны пользователей, оценка защищенности критически важных систем и ресурсов, проведение расследований инцидентов и др. По мере роста потребностей в дополнительных возможностях функциональность данной категории продуктов непрерывно расширяется и дополняется.

Организация резервирования и уничтожения информации

Любая современная ИС должна предоставлять средства резервного копирования, позволяющие восстанавливать базу данных в случае ее разрушения.

Резервное копирование *– периодически выполняемая процедура получения копии базы (массива) данных и ее файла журнала на носителе, хранящемся отдельно от системы.*

Рекомендуется создавать резервные копии базы данных и ее файла журнала с некоторой установленной периодичностью, а также организовывать хранение созданных копий в местах, обеспеченных необходимой защитой. В случае аварийного отказа, в результате которого база данных становится непригодной для дальнейшей эксплуатации, резервная копия и зафиксированная в файле журнала оперативная информация используются для восстановления базы данных до последнего согласованного состояния.

Ведение журнала представляет собой процедуру создания и обслуживания файла журнала, содержащего сведения обо всех изменениях, внесенных в базу данных с момента создания последней резервной копии, и предназначенного для обеспечения эффективного восстановления системы в случае ее отказа. СУБД должна предоставлять средства ведения системного журнала, в котором будут фиксироваться сведения обо всех изменениях состояния базы данных и о ходе выполнения текущих транзакций, что необходимо для эффективного восстановления базы данных в случае отказа.

Преимущества использования подобного журнала заключаются в том, что в случае нарушения работы или отказа СУБД базу данных можно будет восстановить до последнего известного согласованного состояния, воспользовавшись последней созданной резервной копией базы данных и

оперативной информацией, содержащейся в файле журнала. Если в отказавшей системе функция ведения системного журнала не использовалась, базу данных можно будет восстановить только до того состояния, которое было зафиксировано в последней созданной резервной копии. Все изменения, внесенные в базу данных после создания последней резервной копии, будут потеряны.

Резервированию, долговременному хранению подлежат все объекты ЕЦП, оказывающие непосредственное влияние на корректное и безопасное функционирование ЕЦП, а также на обеспечение непрерывности ее работоспособности с целью возможности оперативного восстановления данных объектов за приемлемое время при ликвидации инцидентов ИБ. Сроки резервирования объектов ЕЦП определяются администраторами ИБ.

Для ЕЦП владельцем ИС по согласованию с подразделением по защите информации соответствующего уровня в целях обеспечения возможности восстановления, разрабатывается и утверждается перечень объектов, подлежащих резервному копированию.

Резервные копии объектов ЕЦП при окончании срока хранения должны быть уничтожены физически или с применением специализированных комплексов гарантированного уничтожения информации администраторами ИБ, администраторами ИБ ИС.

Резервированием, восстановлением и уничтожением информации занимаются администраторы, в том числе из состава подразделения по защите информации соответствующих уровней.

Ответственными за резервное копирование объектов ЕЦП являются администраторы. Каждый администратор, в зависимости от его роли и уровня функционирования в ЕЦП, ответственен за определенные объекты копирования, находящиеся на том же уровне в ЕЦП, оказывающие непосредственное влияние на ИБ ЕЦП и функционирование системы защиты информации ЕЦП.

Восстановление объектов из резервных копий проводится администраторами в случае технического сбоя и (или) отказа технических средств или в случае возникновения инцидента ИБ, для устранения

последствий которого необходимо переустановить объекты или перенести их на другое аппаратное обеспечение.

В рамках ЕЦП администраторами ИБ, администраторами ИБ ИС разрабатывается и утверждается перечень объектов, подлежащих долговременному хранению.

Копия долговременного хранения содержит все необходимые индексы, метаданные и управляющие файлы и располагаются на МНИ долговременного хранения.

На МНИ долговременного хранения создаются локальные копии журналов сбора событий, журналов регистрации инцидентов ИБ в целях сокращения окна централизованного резервного копирования и уменьшения нагрузки на ЕЦП, а также перед плановой ротацией и удалением журналов с жестких дисков серверов.

В ЕЦП устанавливаются следующие требования к уничтожению резервных копий объектов на МНИ:

МНИ, содержащие резервные копии объектов, до выдачи их для повторного использования в рамках ЕЦП, должны быть очищены специальным ПО или ОС по согласованию с подразделением по защите информации соответствующего уровня;

МНИ, выводимые из эксплуатации и содержащие резервные копии объектов, распространение и (или) предоставление которых ограничено в соответствии с законодательством в области защиты информации, при выведении из эксплуатации должны быть физически уничтожены;

дальнейшее предназначение (уничтожение или полная очистка) поврежденных МНИ, содержащих объекты, определяется на основе порядка, установленного в МВД.

ГЛАВА 4

ОСНОВЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ

4. 1. Киберпреступность: понятие, сущность и содержание

Сегодня общество перестало воспринимать киберпреступления как невинные проступки или преступление, которое невозможно раскрыть. При этом анализ криминогенной обстановки показывает, что способы и формы совершения киберпреступлений множатся в своем разнообразии. Лидируют среди киберпреступлений преступления корыстной направленности, при их совершении злоумышленники стараются получить доступ к конфиденциальным данным: о клиентах банков, их счетах и финансовых операциях, реквизитах банковских платежных карточек, которые затем можно использовать для хищения денежных средств и др. Все больше преступлений совершается с использованием информационно-коммуникационных технологий. Для преступлений, характерны такие особенности, как использование способов зашифрованного обмена информацией, использование средств анонимизации, криптовалют, что в определенной степени замедляет деятельность правоохранительных органов по установлению преступников. В свою очередь киберугрозы актуальны не только для физических лиц, но и для организаций, поскольку в результате преступных действий они могут пострадать от промышленного шпионажа, утери критически важных данных, в результате их блокирования или удаления, утери контроля над критически важными компьютерными системами.

Внедрение сети Интернет в повседневную жизнь граждан требует своего активного отражения и в деятельности современных правоохранительных органов, которым также надлежит активно использовать достижения технического прогресса в целях решения поставленных перед ними задач. В

этом аспекте необходимо обратить внимание на возможности и сопутствующие проблемы использования сети Интернет для получения ориентирующей и доказательственной информации. Данное направление требует, как технического, так и информационно-методического обеспечения. Вторая составляющая не менее значима по сравнению с технической в свете того, что сотрудники должны иметь представления и знания, например, о функционировании информационно-коммуникационных технологий, сети Интернет и возможностях их использования в служебной деятельности.

Современная реальность такова, что Интернет, предоставляя обширные возможности его использования пользователю: оперирование и обмен информацией удаленно, определенную степень анонимности, оперативность и различные способы использования информации, стал не только орудием правопослушного пользователя, но и в отдельных случаях орудием совершения преступлений.

*Под **киберпреступностью** понимается совокупность преступлений, предусмотренных Уголовным кодексом Республики Беларусь, при совершении которых нарушается состояние защищенности информационной инфраструктуры и содержащейся в ней информации.*

Одним из ключевых проблемных положений дискуссий относительно определения рассматриваемого понятия является вопрос корреляции между киберпреступлением и традиционным преступлением. В качестве критерия, по которому то или иное преступление следует отнести к вышеназванной категории, отдельными авторами предлагается считать возможность совершения данного преступления без использования информационных технологий. Так, например, торговля оружием, может происходить как с использование информационных технологий, так и без них, в то время, как например, хищение имущества путем модификации компьютерной информации без использование информационных технологий невозможно.

Киберпреступления характеризуются следующими особенностями:

трансграничный характер киберпреступлений, при котором злоумышленник, объект преступного посягательства и потерпевший могут находиться на территорий различных государств;

дистанционный характер преступных действий в условиях отсутствия физического контакта преступника и потерпевшего;

определенная подготовленность преступников;

интеллектуальный характер преступной деятельности;

в отдельных случаях возможность совершения преступления в автоматизированном режиме в нескольких местах одновременно;

в отдельных случаях неосведомленность потерпевших о том, что они подверглись преступному воздействию.

Анализ практики деятельности ОВД показывает, что **по направлению «противодействие киберпреступности» подлежат учету преступления, такие, например, как:**

К первой группе киберпреступлений относятся преступления против компьютерной безопасности:

несанкционированный доступ к компьютерной информации;

уничтожение, блокирование или модификация компьютерной информации;

неправомерное завладение компьютерной информацией;

разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств;

нарушение правил эксплуатации компьютерной системы или сети.

Также по данному направлению учитываются преступления против общественного порядка и общественной нравственности, против человека, а именно: заведомо ложное сообщение об опасности.

Ко второй группе киберпреступлений, относятся совершаемые против собственности:

вымогательство и мошенничество, если их совершение сопряжено с совершением преступлений против компьютерной безопасности;

хищение путем модификации компьютерной информации;

причинение имущественного ущерба без признаков хищения, если ущерб в результате преступления причинен путем модификации компьютерной информации.

К третьей группе относятся преступления против порядка осуществления экономической деятельности, в частности, незаконный оборот средств платежа и (или) инструментов.

В свою очередь, выделяется несколько направлений понимания *роли сети Интернет в совершении преступлений:*

среда совершения преступлений;

способ совершения преступлений;

средство совершения традиционных преступлений;

средство подготовки и сокрытия следов совершаемого преступления.

Первый подход относится в большей степени к совершению преступлений, подпадающий под компетенцию подразделений по противодействию киберпреступности, остальные же характеризуются в большей степени универсальностью и применимостью к множеству преступлений.

В литературе встречаются различные классификации киберпреступлений, например, *по характеру использования компьютерных систем и сетей выделяют следующие виды*:

преступления, при совершении которых средства компьютерной техники выступают как орудия совершения преступления;

преступления, при совершении которых средства компьютерной техники выступают как предмет преступного посягательства;

преступления, так или иначе связанные с использованием средства компьютерной техники.

Деятельность правоохранительных органов по предупреждению, выявлению, пресечению киберпреступлений носит сложный, многогранный характер и требует применения значительного объема специальных знаний и соответствующих научно-технических средств.

В настоящее время актуальны следующие формы совершения киберпреступлений: вишинг; фишинг; фарминг; кардинг; заражение вредоносным программным обеспечением; ddos-атаки; сваттинг.

Вишинг (телефонный фишинг) *– вид киберпреступления, при котором злоумышленник, используя телефонную коммуникацию и играя определённую*

роль (например, сотрудника банка и др.), под разными предлогами выманивают у держателя банковской платежной карточки конфиденциальную информацию или стимулируют к совершению определённых действий со своим банковским счетом (банковской платежной картой), с целью хищения денежных средств.

При совершении киберпреступлений злоумышленниками активно используется социальная инжинерия.

Социальная инженерия *– это совокупность способов психологического воздействия на поведение человека с целью получения выгоды.*

Злоумышленники, используя телефонную связь и выдавая себя за сотрудников банков, под различными предлогами выясняют у потерпевших сведения о наличии банковских платежных карточек, сроках их действия, CVV (CVC)-кодах, паспортных данных, смс-кодах с целью хищения денежных средств. В ряде случаев злоумышленникам известны некоторые реквизиты БПК, а также персональные данные лиц, на имя которых они эмитированы.

В отдельных случаях при совершении звонков потерпевшим преступники используют IP-телефонию[6].

IP-телефония *– это технология, которая обеспечивает передачу голоса в сетях с пакетной коммутацией по протоколу IP, частным случаем которых является сеть Интернет.* Другими словами, обеспечивает осуществление соединений и голосового общения из специальных приложений для персональных компьютеров и мобильных устройств с абонентами мобильных и стационарных телефонных сетей.

VoIP (Voice over Internet Protocol) *– протокол, предназначенный для передачи голоса на базе пакетов в IP-сетях.*

Основными компонентами VoIP-соединения являются:

терминал;

шлюз;

[6] Принятие правоохранительными органами мер профилактического характера (разъяснительных, организационных, технических) позволило сократить использование рассматриваемой технологии в преступных целях.

контроллер зоны (привратник) – выполняет функцию управления зоной сети IP–телефонии, зарегистрированные у этого привратника. Выполняет преобразование адреса (телефонного номера) в IP-адрес сетей.

контроллер управления многоточечной конференции (MCU — MultipointControlUnit).

Ключевыми потребителями услуг IP-телефонии являются крупные организации, которые желают минимизировать затраты на телефонные переговоры. Предоставляют данные услуги ряд организаций, например, «E2 Phone» (Королевство Нидерланды), «Ventatel Limited» (Республика Кипр), «Nova Metro» (Эстонская Республика) и другие. Для заказчиков посредством IP-телефонии создаются своеобразные мини-АТС с внутренними идентификаторами абонентов (они могут содержать не только цифры, но и буквы и другие символы) с возможностью осуществления звонков как внутри сети, так и на внешние абонентские номера.

Облачная АТС (виртуальная АТС) *– корпоративная телефонная станция, размещенная на хостинге и предоставляемая компании как облачный сервис для организации офисной телефонии, а также инструмент для налаживания процесса продаж, улучшения клиентского сервиса и оптимизации бизнес-процессов.*

Учитывая, что инициатор вызова при таком соединении не использует обычную телефонную сеть (приложение может быть установлено на персональном компьютере или мобильном устройстве даже без сим-карты), у принимающего абонента отображается не абонентский номер телефонной сети, а именно установленный **идентификатор IP-телефонии**. Данная особенность IP-телефонии используется преступниками, которые заказывают у соответствующих организаций комплекс услуг IP-телефонии с выбором в качестве внутренних идентификаторов номеров, набор цифр в которых соответствует или схож с абонентскими номерами телефонных сетей. Такие номера отображаются на дисплеях мобильных устройств и фиксируются компаниями мобильной (стационарной) телефонной связи. Важно понимать, что, скорее всего, они не являются абонентскими номерами (таких номеров

может не существовать либо ими могут пользоваться люди, которые не причастны к преступной деятельности).

В настоящее время сформирована индустрия мобильного банкинга, интернет-банкинга и хорошо развиты технологии IP-телефонии. Это позволяет преступникам создавать подпольные колл-центры по «обзвону» граждан для совершения хищений.

Также могут использовать мессенджеры (например, Viber, WhatsApp и др.) в которых существует возможность использования виртуальных номеров. После регистрации таких номеров в мессенджерах, преступники осуществляют звонки гражданам и под различными предлогами пытаются получить у них различные сведения.

Так, например, в ОВД обращаются граждане, которым звонят на номер сети оператора сотовой связи либо же звонок поступил в приложении одного из мессенджеров. Звонивший представляется работником банка (правоохранительных органов) и сообщает, что с денежными средствами держателя карты неизвестный пытается произвести финансовые операции. Чтобы предотвратить вывод денег, звонивший требует назвать ему данные карты: номер, CVV-код, срок действия, пик-код и др. Многие от растерянности, по незнанию и по ряду других причин сообщают преступнику реквизиты и как следствие лишаются средств со счета.

С целью установления является ли номер, с которого поступил звонок, абонентским номером телефонной сети или идентификатором IP-телефонии, необходимо направить запрос (запросы) в соответствующие телекоммуникационные организации.

В свою очередь *преступниками возможна реализация получения доступа к учётным записям месенджеров.* Например, получение доступа учетной записи пользователя мессенджера «Viber», которая затем используются для совершения преступлений. Получение доступа возможно посредством использования десктопного приложения данного мессенджера, установленного на персональный компьютер (далее – ПК). После осуществления установки данного программного обеспечения, предлагается осуществить копирование данных с мобильного устройства где установлено мобильное приложение

«Viber» на ПК. Осуществление указанных действий возможно путём сканирования QR-кода камерой мобильного устройства или создания ссылки активатора, создаваемой путём выбора пункта «Не работает камера?». После осуществления второго действия, пользователь получает ссылку, содержащую информацию о ключе идентификаторе ПК, на котором будет осуществлена активация мессенджера «Viber». Злоумышленник, получив указанную ссылку, может осуществить её рассылку посредством любых мессенджеров (электронной почты) передачи данных. После осуществления перехода по указанной ссылке, пользователь мессенджера «Viber» осуществит переход в указанный мессенджер, где получит системное уведомление содержащие в себе текст согласия на активацию «Viber» на другом устройстве. Также в указанном уведомлении присутствует виртуальная кнопка «Разрешить», которая становиться активной для нажатия только после простановки разрешения об активации. После осуществления нажатия виртуальной кнопки «Разрешить», учётная запись копируется на устройство, посредством которого была сгенерирована вышеуказанная ссылка. Одновременно с этим, пользователю мобильного устройства показывается информационное окно с кнопкой «Синхронизация», посредством которой (при её нажатии) будет осуществлена синхронизация контактов и сообщений между мобильным устройством и ПК, на котором дополнительно активирован «Viber». По окончанию синхронизации пользователь будет уведомлён о проведении указанных действий путём отображения соответствующего сообщения. Таким образом, пользователь добровольно предоставляет данные лицу, которое неправомерно завладевает информацией[7]. Преступники постоянно пытаются обнаружить различные новые уязвимости, в том числе в мессенджерах и социальных сетях, чтобы использовать их для совершения преступлений

Фишинг *– вид киберпреступления, целью которого является получение доступа к конфиденциальным данным пользователей (логинам, паролям), путем создания электронных писем от чужого имени или веб-страниц похожих, либо полностью повторяющих настоящие, которым жертва может*

[7] Принятие правоохранительными органами мер профилактического характера (разъяснительных, организационных, технических) позволило сократить использование рассматриваемой технологии в преступных целях.

довериться по невнимательности, как правило, с целью последующего хищения денежных средств.

Сюда можно отнести хищение паролей, данных платежных карт, банковских счетов и иной конфиденциальной информации. В отличие от других киберугроз, фишинг не требует наличия глубоких технических знаний. Фишинговые преступники не пытаются воспользоваться техническими уязвимостями в операционной системе устройства, они прибегают к методам социальной инженерии.

Фишинговые схемы могут быть различные, предлоги, под которыми преступники получают данные, постоянно меняются. Так, например, может реализовываться способ, связанный с покупками и продажами в сети Интернет. В чатах мессенджеров распространяется ссылка на продажу, например, бытовой техники. Переходя по ней, предлагается оплатить покупку на сайте, где предусмотрена форма для ввода реквизитов банковской платежной карточки (адрес фишингового сайта может отличается от оригинала всего одним символом). После ввода реквизитов банковской платежной карточки денежные средства со счета похищаются.

Также с помощью мессенджера или электронной почты может осуществляться рассылка, например, с текстом «Вам поступил денежный перевод», «Изменился порядок оплаты налогов. Для получения инструкции переходите по ссылки» Если получатель письма переходит по ссылке, затем вводит на сайте свои данные, мошенники получают доступ к данным персонального компьютера или телефона, либо может осуществляться заражение ВПО. После этого осуществляется доступ к аккаунтам в социальных сетях, к реквизитам банковских платежных карточек, паролям от интернет-банкинга с целью последующего совершения хищения.

Можно выделить следующие виды фишинга:

почтовый (с использованием рассылки электронных сообщений. Основан на использовании вредоносного программного обеспечения, а также установленных на компьютере пользователя спам-фильтров. Кроме того, могут отсылаться сообщения якобы с официальной страницы банка),

онлайновый (с использованием копирования страниц онлайн-банкинга известных банков. Подменяется страница используемого онлайн-банкинга на поддельную, которая внешне является двойником оригинала. Когда пользователь заходит на такую страницу и вводит логин и пароль, они становятся доступны преступникам);

комбинированный. При комбинированном «фишинге» создается поддельный сайт банка, пользователям предлагается самостоятельно произвести некоторые операции. От имени банка также направляются сообщения с целью ознакомления с новыми привлекательными банковскими продуктами. При этом предлагается пользователю перевести средства со своего счета на депозит, якобы открытый для него банком. Получив таким образом доступ к счету жертвы, преступники переводят деньги с него на свои счета.

Информацию об интернет-сайте, используемом в преступной деятельности, можно получить у хостинг-провайдера (хостера), на сервере которого размещен сайт, и у регистратора, зарегистрировавшего доменное имя данного сайта. Часто (но не всегда) хостер и регистратор – одна и та же организация, представленная сайтом в сети Интернет.

Фарминг *– разновидность фишинга, заключающаяся в перенаправлении пользователя на сторонние интернет-ресурсы.*

Происходит подмена настоящего интерен-ресурса на мошеннический, позволяющий злоумышленнику получить конфиденциальные данные пользователя, посредством использования кэша DNS на конечном устройстве пользователя или же на сетевом оборудовании провайдера. После осуществления подмены злоумышленник рассчитывает на авторизацию пользователя на интернет-ресурсе и получение его данных. Фарминг-программы могут работать как из кэша браузера, так и непосредственно в виде вредоносного программного обеспечения на персональном компьютере, которое активизирует свою деятельность в момент перехода на интересующую страницу (интернет-банкинг и т.п.).

Кардинг – *противоправная деятельность в сфере оборота банковских платежных карт и их реквизитов, связанная с хищением денежных средств.*

Условно подразделяется на реальный и вещевой кардинг. Основывается на компрометации данных банковской платежной карты. Наиболее широко этот вид хищения был распространен до перевода банковских платежных карточек на чиповые технологии. Также возможна компрометация реквизитов карточки для совершения операций без ее непосредственного использования (оплата в сети Интернет).

Реальный кардинг заключается в использовании информации с чужой банковской платежной карточки в терминалах. **Вещевой кардинг** нацелен на приобретение товаров, подарочных сертификатов, подписок, услуг и т.д., используя чужие банковские реквизиты.

Заражение вредоносным программным обеспечением *– внедрение злоумышленниками специализированного программного обеспечения в компьютерную систему пользователя для хищения его конфиденциальных данных, завладения ценной информацией, шифрования данных с требованием выкупа, использования компьютера или иного устройства в специализируемых сетях с целью совершения иных преступлений.*

ВПО – программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самого компьютера или к хранимой информации, с целью несанкционированного использования его ресурсов или причинения вреда владельцу компьютера (информации), компьютерной сети. ВПО создается для несанкционированного блокирования, модификации, уничтожения или копирования информации, нарушения работы компьютеров или компьютерных сетей.

Наиболее распространенные виды вредоносного программного обеспечения, используемые при совершении преступлений: вирус, червь, троян (бэкдор, загрузчик, руткит, программы-вымогатели, эксплойт).

Черви *представляют собой общий класс вредоносного программного обеспечения, характеризующийся самовоспроизводством.* Однако черви не могут заражать существующие файлы, они внедряются в компьютер отдельным файлом и ищут уязвимости в сети или системе для своего дальнейшего распространения. Черви также могут подразделяться по способу заражения (электронная почта, мессенджеры, обмен файлами и пр.) и нацелены на

определенную уязвимость (уязвимости). Сканируя системы, которые подвержены этой уязвимости, эксплуатируют систему, копируют в нее свой код и начинают сканирование заново для обнаружения других жертв. Черви могут распространяться за считанные минуты, что обусловлено их автоматической природой. Некоторые черви существуют в виде сохраненных на жестком диске файлов, а некоторые – в оперативной памяти компьютера.

Троян *по своему действию является противоположностью вирусам и червям, не самовоспроизводятся и не распространяются сами по себе.* Загружаются под видом обычного приложения, однако вместо заявленной функциональности, выполняют задачи, запланированные злоумышленниками. Трояны эволюционировали до таких сложных форм, как, например, бэкдор (удаленное администрирование) и загрузчик (устанавливает на компьютер вредоносный код).

Бэкдор *– это программное обеспечение, которое позволяет удаленно управлять компьютером как законному системному администратору, так и злоумышленнику, т.е. средство удаленного администрирования.*

Бэкдоры позволяют выполнять различные функции: отправлять, принимать или уничтожать файлы, запускать программное обеспечение, удалять информацию, перезагружать компьютер, включать микрофон или камеру, также они используются для объединения компьютеров-жертв в так называемые ботнеты – сети «зараженных» компьютеров, централизованно управляемых злоумышленниками. По своей функциональности они во многом напоминают различные системы администрирования, разрабатываемые официальными производителями программного обеспечения.

Загрузчик *– часть кода, используемая для загрузки и установки полной версии «вредоноса».* После того как загрузчик попадает в систему путем сохранения вложения электронного письма или, например, при просмотре зараженной картинки, он соединяется с удаленным сервером и загружает весь «вредонос».

Программы-вымогатели *являются вредоносным программным обеспечением, шифрующим данные с помощью ключа, известного только злоумышленникам.* Для получения ключа, необходимый для расшифровки и

восстановления данных, предлагается произвести оплату. Если выкуп не выплачивается вовремя (обычно в криптовалюте), данные удаляются или просто блокируются и становятся недоступными для пользователя.

Руткит *представляет собой часть вредоносных программ, разработанных специально для того, чтобы скрыть присутствие вредоносного кода и его действия от пользователя и установленного защитного программного обеспечения.* Руткит ничего вредоносного не делает, однако в большинстве случаев используется другим вредоносным программным обеспечением для затруднения собственного обнаружения. Скрывает в системе определенные объекты либо активности, как правило, ключи реестра (например, отвечающие за автозапуск вредоносных объектов), процессы в памяти зараженного компьютера, вредоносную сетевую активность. Это возможно благодаря тесной интеграции руткита с операционной системой, некоторые руткиты могут начать свою работу прежде, чем загрузится операционная система (буткиты).

Эксплойт *– компьютерная программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему (целью атаки может быть получение контроля над системой, так и нарушение её функционирования).*

Как правило используются для проникновения на компьютер с целью последующего внедрения туда вредоносного кода (например, заражение всех посетителей взломанного веб-сайта вредоносной программой). Также эксплойты интенсивно используются программами для проникновения на компьютер без участия пользователя.

Необходимой для киберпреступников задачей является внедрение вируса, червя или троянской программы в компьютер или мобильный телефон. Достигается эта цель различными способами, которые делятся на две основные категории:

социальная инженерия;

технические приёмы внедрения в заражаемую систему без ведома пользователя.

Часто эти способы используются одновременно. Метод социальной инженерии – для привлечения внимания потенциальной жертвы, а технический – для увеличения вероятности проникновения заражённого объекта в систему. Скрытное внедрение вредоносного кода осуществляется через уязвимости в системе безопасности операционных систем и в программном обеспечении. Наличие уязвимостей позволяет изготовленному вредоносному программному обеспечению проникнуть в компьютер и самостоятельно запустить себя на исполнение. Уязвимости являются ошибками в коде или в логике работы различных программ, современные операционные системы и приложения имеют сложную структуру и широкий функционал, поэтому избежать ошибок при их проектировании и разработке просто затруднительно. Этим и пользуются вирусописатели и компьютерные злоумышленники.

Вредоносное программное обеспечение для мобильных устройств несравнимо по сложности с аналогами для персональных компьютеров, ниже представлены некоторые самые популярные его типы:

вредоносное банковское программное обеспечение. Количество вредоносных мобильных программ, нацеленных на сервисы онлайн-банкинга растет;

мобильные программы-вымогатели, которые блокируют данные пользователя, такие как документы, фотографии и видео, зашифровывают эту информацию, а затем требуют выкуп за ее расшифровку;

мобильное шпионское программное обеспечение, которое отслеживает активность пользователя, регистрирует местоположение и изучает информацию, такую как имена пользователей, пароли к аккаунтам электронной почты или сайтам интернет-магазинов. Его присутствие остается незаметным для пользователя до тех пор, пока не снизится производительность устройства в силу дефицита системных ресурсов, или не будет запущена программа-антивирус.

Вредоносное программное обеспечение стало более доступно, в сети Интернет можно найти вредоносные инструменты (например, добровольно раскрытый исходный код, или разработанный кибергруппами прошлого, или легальные программные решения для тестирования на проникновение).

Отдельно стоит отметить сетевые атаки, которые используют определенные ограничения пропускной способности, которые характерны для любых сетевых ресурсов, например, инфраструктуре, которая обеспечивает условия для работы интернет-сайта организации.

DoS *– хакерская атака на вычислительную систему проводимая с одиночного компьютера с целью довести её до отказа, то есть создание таких условий, при которых добросовестные пользователи системы не смогут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ будет затруднён.*

DDoS – *хакерская атака на вычислительную систему, заключающаяся в подавлении веб-ресурса или сервера трафиком из огромного количества источников, с целью доведения до отказа в обслуживании.*

DDoSатаки основаны на том, что они могут отправлять больше данных, чем способен поддерживать канал интернет-провайдера жертвы. Одним из ресурсов, на которые чаще всего посягают злоумышленники, является пропускная способность компьютерной сети. Большие объемы данных отправляются на один сервер с целью превышения доступной пропускной способности, если вся пропускная способность занята трафиком, формируемым злоумышленниками, то легитимный трафик не может быть доставлен, и сервер не может отправлять ответы другим пользователям. Чтобы обеспечить максимальное снижение пропускной способности, эти типы атак обычно распространяются на несколько систем; при этом атака идет на одну цель, поэтому они и называются атаками с распределенным отказом в обслуживании (DDoS).

В свою очередь на территории Республики Беларусь фиксируется рост поступления заведомо ложных сообщений об опасности, так называемого «сваттинга» («лжеминирований»).

Данный вид противоправной деятельности набирает обороты в сети Интернет. При этом, наибольшее распространение имеет среди лиц школьного возраста, как инструмент мести обидчику или, например, срыва нежелательных занятий в учебном заведении.

В своей реальной сущности «сваттинг» представляет собой тактику введения правоохранительных и иных государственных органов в заблуждение (например, путем направления электронного письма, содержащего заведомо ложные сведения такие как установка взрывного устройства, захват заложников др.) с целью, чтобы по указанному адресу были направлены наряды (спецподразделения) органов внутренних дела, органов по чрезвычайным ситуациям. Сообщения об опасности, такие как минирование зданий или захват заложников, являются преступлением, которое может привести к огромным издержкам, таким как эвакуация людей из зданий, задержание подозрительных лиц, перекрытие улиц, задержка транспортных рейсов. Возникновение подобных ситуаций требует незамедлительного реагирования, вплоть до введения мероприятий в рамках специальных планов, на любые сообщения об опасности, в которых содержатся сведения об угрозе жизни людей, однако, в некоторых случаях такая оперативность играет, наоборот, на руку злоумышленников и подстрекает их к новой рассылке заведомо ложных сообщений.

Согласно сведениям МВД Республики Беларусь из всех зарегистрированных заведомо ложных сообщений об опасности, только часть сообщений содержали в себе признаки «сваттинга» (сведения о каком-либо лице, которому злоумышленник желал доставить неудобства, связанные с выбытием следственно-оперативной группы), а большинство сообщений содержали только текст с формулировками, связывающими их направление с геополитическими событиями (проводимой Российской Федерацией специальной военной операцией на территории Украины) или с общественно-политическими событиями в Республике Беларусь. Сообщения, как правило, содержали заведомо ложные сведения о размещении взрывных устройств на критически важных объектах инфраструктуры, социально-значимых учреждениях и местах большого скопления людей (железнодорожные пути, железнодорожные вокзалы, учреждения образования, крупные предприятия и торговые центры).

Изучение практики противодействия данному виду преступлений позволяет сделать вывод о психологическом потрете лица, совершающего

«сваттинг». Как правило, это лица в возрасте от 14 до 20 лет, проводящие большую часть времени в глобальной сети Интернет, с плохой социальной адаптацией, выражающейся в отсутствии реальных дружеских связей, а также возможными психологическими отклонениями (психологические отклонения официально были задокументированы у нескольких лиц), выражающимися в навязчивой идее самоутверждения в обществе, путём обретения популярности, либо создании вокруг себя культа личности с мнимыми последователями.

Зачастую заведомо ложные сообщения об опасности состояли из заранее заготовленных шаблонов, так называемых «сборных текстовых конструкций», содержащих весь спектр сведений, необходимых, по мнению злоумышленников, для обязательного реагирования правоохранительной системы Республики Беларусь. Рассылка таких сообщений носит массовый (веерный) характер, что указывает на целенаправленные и скоординированные действия злоумышленников по дестабилизации ситуации в сфере общественной безопасности в стране. При этом зачастую в тексте сообщений не используется буква «ы», отсутствующая в украинском языке и раскладке клавиатуры, или вместо неё применяется написание буквы «и», сочетаний символов «ь» и «і» (ьі).

Как правило, злоумышленниками для осуществления рассылки заведомо ложных сообщений, используются иностранные (преимущественно западных стран) почтовые сервисы, такие как «Gmail», «Protonmail», «Mailfence», «Hey», и д.р., что создаёт сложности при получении сведений об отправителе, поскольку осуществляется в рамках международного сотрудничества.

Заведомо ложные сообщения с признаками «сваттинга» отличаются наличием обширных возможностей для проведения оперативно-розыскных мероприятий, поскольку в самом сообщении уже содержатся значимые идентификаторы.

Наиболее распространёнными идентификаторами, указываемыми в сообщениях, являются:

ссылки на личные страницы в социальных сетях;

абонентские номера;

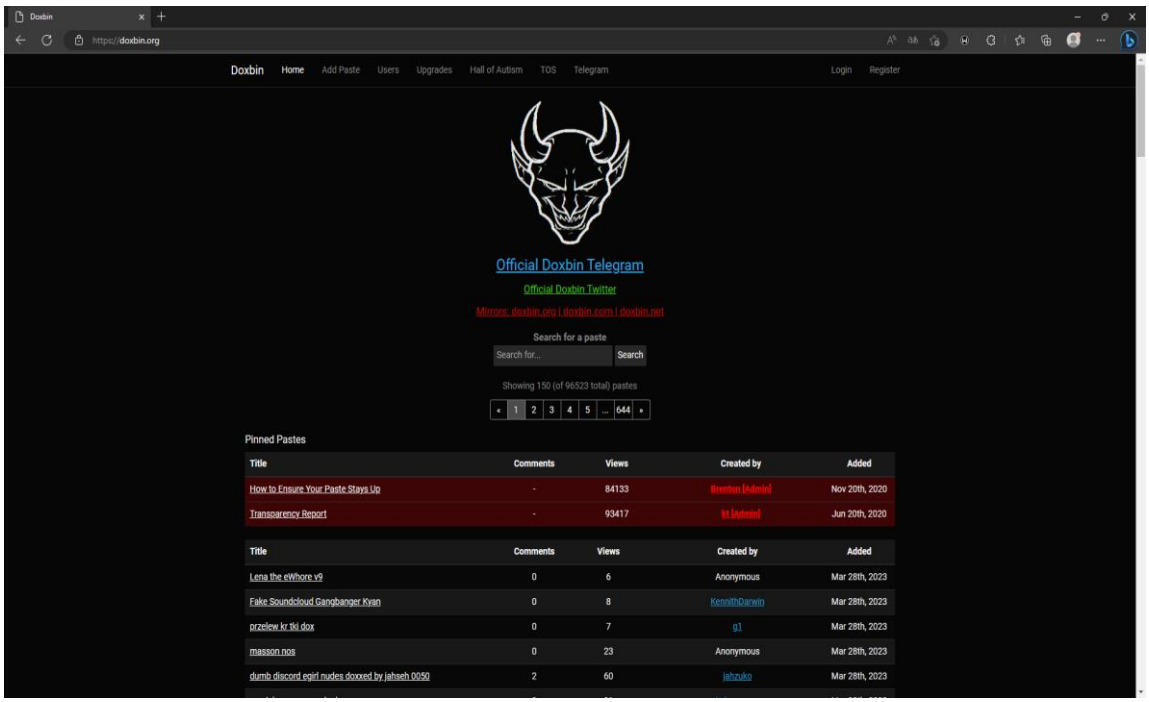
реальные данные лица (написание письма от имени конкретного человека) – редко;

адреса криптокошельков;

косвенные сведения о лице (имя и место учёбы, никнейм в компьютерной игре).

Важным аспектом получения значимой информации является наличие у сотрудника навыков поиска информации по открытым источникам в глобальной сети Интернет, а также умения построить диалог с данными лицами в ходе виртуального общения (опроса). Любой пользователь сети Интернет в ходе повседневного пользования мобильным телефоном или персональным компьютером оставляет за собой ряд идентификаторов, таких как: никнейм, имя, номер телефона, адрес электронной почты, фотография, публичные переписки и участие в сообществах, а также иные сведения (включающие в себя публичные данные пользователя, технические сведения, а также результат их анализа).

Следует отметить интернет-ресурс https://doxbin.org/, который пользуется популярностью среди лиц, занимающихся рассылкой заведомо ложных сообщений об опасности. Данный ресурс представляет собой информационную стену, на которой пользователи размещают информацию об иных пользователях, занимающихся противоправной деятельностью в глобальной сети Интернет, в том числе, «сваттеры» размещают на данном ресурсе сведения о своих жертвах, а также о других «сваттерах» с которыми у них произошёл конфликт.



Интернет-ресурс https://doxbin.org

Касаясь тенденций в сфере противодействия киберпреступности необходимо отметить, что происходит сокращение численности киберпреступных групп, что обусловлено удорожанием уязвимостей, переходом на облачные серверы и появлением доступных готовых инструментов для совершения кибератаки.

Киберпространство используется для структурной оптимизации криминальных формирований. Многие преступные группы организуются на основе сетевого принципа как временный союз для решения конкретной криминальной задачи. При этом в преступных действиях может участвовать широкий круг лиц, находящихся территориально в разных государствах. Нередко группа приобретает транснациональный характер, в такой группе может отсутствовать лидер, участники группы могут быть лично незнакомы, а координация деятельности осуществляется с использованием сетевых технологий. Преступные группы, построенные по сетевому принципу, приобретают высокую адаптивность к изменениям в среде существования и устойчивость к внешним воздействиям за счет: гибкого управления и повышенной скорости реагирования на действия правоохранительных органов,

отсутствия четко локализуемой структуры, способности к быстрым изменениям состава и перераспределению ролей.

Киберпреступные группы становятся более гибкими. Например, администраторы для обслуживания физической инфраструктуры больше не нужны, так как облачные сервисы упростили этот аспект. Злоумышленники могут не создавать собственное ВПО, если раньше крупным группам требовались специалисты для разработки разных частей программы (например, клиентской и серверной), то теперь достаточно одного оператора. Длинные цепочки атаки, включающие эксплойты для разных уязвимостей, стали короче, таким образом, создатели эксплойтов, которые специализировались на клиентской части, стали менее востребованными.

Таким образом, *для проведения атаки в киберпреступной группе присутствует:*

организатор (руководитель);

оператор вредоносного программного обеспечения;

специалист, который обеспечит доступ к сети;

специалист по финансам (вывод и обналичивание похищенных финансовых средств).

В свою очередь, цели преступников не ограничиваются финансовыми организациями. С появлением ботнетов образовался рынок данных для доступа к корпоративным сетям. Преступники стали взламывать компании, работающие в самых разных отраслях с целью продажи в теневом интернете доступ к их активам. Отдельные организации перевели часть инфраструктуры в сеть Интернет и организовали удаленный доступ для сотрудников, тем самым увеличив поверхность кибератаки и расширив возможности преступников для входа в компьютерные сети.

Тенденцией является то, что в область интересов преступников, попадают пользователи (физические лица и организации), которые осуществляют криптовалютные операции и владеют криптовалютой (например, криптообменники, криптокошельки и др.).

Многие услуги по-прежнему востребованы и доступны на теневом рынке:

продажа учетных записи (для пользования преступниками онлайн-сервисами (например, облачными) необходимы электронные адреса, номера телефонов.

доступ к аккуантам (помимо обычных комбинаций номера телефона и адреса электронной почты, преступники продают украденные данные от игровых, стриминговых, банковских и других аккаунтов. Эту информацию можно использовать в самых разных целях — от мошенничества до вывода денежных средств).

проведение DDoS-атаки;

продажа персональных данных (информация о пользователях: номера банковских платежных карт, паспортные данные, данных для доступа к банковским счетам и др.).

Данные по-прежнему остаются ценным активом, несмотря на значительные усилия по их защите личная информация пользователей по-прежнему утекает в сеть Интернет и используется для кибератак, так, например, с ее помощью преступники, могут зарегистрировать сервер или получить доступ к корпоративной сети.

Современное состояние развития общества и экономики характеризуется существенным увеличением доли безналичного денежного оборота в общем объеме финансовых транзакций, что обусловлено активным внедрением различных систем расчетов с использованием электронных средств платежа[8] (далее – ЭСП). К ним относится широкий перечень средств оплаты товаров и услуг или денежных переводов: платежные карты, мобильные устройства и персональные компьютеры с доступом к банковским счетам и аккаунтам, электронные платежные системы и системы дистанционного банковского обслуживания «Клиент-банк» (далее – ДБО).

По мере роста количества и сумм безналичных операций возросло и количество противоправных деяний в отношении владельцев денежных средств. Особую общественную опасность представляют мошеннические

[8] Здесь и далее под электронным средством платежа понимается средство и/или способ, которые позволяют клиенту оператора по переводу денежных средств составлять/удостоверять/передавать распоряжения для перевода денежных средств в рамках применяемых форм безналичных расчетов с использованием информационно-коммуникационных технологий, электронных носителей информации (в том числе платежных карт), а также других технических устройств.

действия, отличающиеся от других имущественных преступлений тем, что потерпевший добровольно отдает свое имущество преступнику вследствие обмана или злоупотребления доверием, которые вводят жертву в заблуждение. Используя методы социальной инженерии, основанные на достижениях современных информационных технологий, преступники выманивают у пользователей необходимые для осуществления незаконных платежей или переводов реквизиты (например, сеансовые пароли, используемые для подтверждения клиентом согласия на совершение операций с помощью мобильных приложений, пароли защищенного протокола авторизации «3-D Secure»), либо осуществляют несанкционированный доступ к пользовательской информации, позволяющие выполнить авторизацию и последующее хищение денежных средств со счетов пользователей

Основными тенденциями совершаемых хищений в рассматриваемой сфере[9] *являются:*

увеличение количества преступлений с использованием социальной инженерии (фишинг, вишинг, взлом учетных записей пользователей в социальных сетях);

звонки в результате утечки персональных данных, например, на маркетплейсах;

наличие фактов компрометации системы ДБО клиентов в рамках социальной инженерии, в результате чего преступники получают учетные данные (логины, пароли и ключи) доступа к системе ДБО;

мошенничество по токенам, когда преступники с использованием социальной инженерии выманивают не только реквизиты платежной карты и «3-D Secure» пароль, но и данные, необходимые для присвоения токена к платежной карте, привязывают токен держателя на свое мобильное устройство. В настоящее время «3-D Secure» является самым распространенным методом дополнительной проверки;

[9] По данным ОАО «Банковский процессинговый центр» (специализированный центр по информационно-технологическому обеспечению безналичных расчетов с использованием банковских платежных карт отечественной платежной системы и международных систем, действующих на территории Республики Беларусь).

рассылка в социальных сетях уведомлений о выигрышах, когда держатели сами вводят реквизиты платежных карт для получения выигрыша;

увеличение количества преступных операций на онлайн-сервисах, которые занимаются продажей цифровых товаров: компьютерных игр и программного обеспечения (взлом аккаунтов учетной записи Google, после осуществляются операции оплаты Google сервисов в пределах остатка баланса на счете);

присутствие фактов «friendly fraud» мошенничества. Например, когда злоумышленником в интернет-магазине заказывается и оплачивается товар, а затем происходит убеждение продавца совершить возврат денежных средств, мотивируя тем, что произошло хищение банковской платежной карты, взлом электронного кошелька или используется другой повод с целью возмещения денежных средств, при этом предпринимается попытка оставить товар;

вещевой кардинг;

смещение хищений с использованием электронных платежных инструментов и сервисов все больше в сферу электронной коммерции.

Также специалистами отмечается, что в ближайшей перспективе будут актуальны следующие способы совершения рассматриваемых преступлений:

с использованием социальной инженерии, что будет актуально до повышения уровня финансовой цифровой грамотности пользователей;

перехват доступа к интернет-банкингу, что предоставляет преступнику получение доступа ко всем платежным картам и счетам, появляется возможность открывать кредитные линии;

использование шифровальщиков, когда трояны-вымогатели, блокируют доступ к данным и требуют определённую сумму для возвращения доступа к информации;

использование банковских банковский «троянов»;

компрометация межбанковской системы идентификации;

атаки на сотрудников, работающих удалённо, поскольку преодоление систем защиты вне корпоративной сети осуществляется легче;

более активное использование искусственного интеллекта, например, для создания дипфейков, повышения эффективности вредоносного программного

обеспечения, преодоление защиты «captcha», подбора паролей, анализа больших массивов данных с целью извлечения номеров телефонов и реквизитов платежных карт.

Наиболее распространёнными инструментами электронных средств платежа являются технологии онлайн-платежей на основе: банковских платежных карт; электронных денег; интернет-банкинга (система ДБО).

Обращение электронных денег осуществляется в сети Интернет, их можно использовать при помощи электронных (виртуальных кошельков), интернет-банкинга, устройств, работающих с банковскими платежными картами и др. Интернет-банкинг является технологией дистанционного банковского обслуживания (далее – ДБО), позволяющей осуществлять управление счетами с использованием компьютерной сети Интернет, а также предоставлять посредством программно-аппаратных средств и компьютерной сети Интернет банковские услуги. Получение доступа к системе ДБО возможно посредством портативного устройства и персонального компьютера с использованием специального приложения (программного обеспечения) или браузера (web-клиента).

При совершении преступлений злоумышленники досконально изучают особенности функционирования электронных средств платежа, в том числе программно-техническое обеспечение, с целью использования различных технологических особенностей в преступных целях, устанавливают уязвимости, которые используют при совершении хищений. После чего возможна разработка соответствующего программного обеспечения, либо его приобретение на специализированных интернет-ресурсах, в том числе в Даркнете. Эксплуатируя выявленную уязвимость или технологическую особенность похищаются денежные средства и перемещаются на счета, контролируемые преступниками (например, используются дропы и др.), после чего осуществляется их вывод с указанного счета и обналичивание.

Основными участниками технологии онлайн-платежей могут являться:

покупатель (владелец счета, электронных денег и др.);

продавец (например, интернет-магазин, предприятие торговли (услуг);

платежная система;

платежный агрегатор;

платежный шлюз;

эмиссионный банк;

банк-эквайер;

процессинговый центр.

Например, совершая платеж покупатель вводит платежные данные через веб-интерфейс сайта интернет-магазина, после чего информация передается через платежный шлюз в банк-эквайер, который отправляет запрос на платеж в платежную систему, получает запрос на авторизацию, отправляет этот код назад в платежную систему, которая совершает операцию, код авторизации возвращается в платежный шлюз, а также этот же код уходит в интернет-магазин с результатом операции.

Для использования электронных средств платежа на компьютер или мобильный телефон может устанавливаться специально предназначенное для этого программное обеспечение, которое поддерживает ведение локально или удаленно электронного (виртуального кошелька), который можно пополнить денежными средствами (например, банковский, почтовый перевод), а также за счет перечисления из других кошельков. Электронный (виртуальный) кошелек – это специальное программное обеспечение, которое необходимо для учета и управления электронной наличностью, как правило, представляет собой сложный код, отражающий состояние денег в системах. Электронные платежные системы являются составной частью отношений банк-клиент и в обобщенном виде в любых электронных расчетах за владельцами электронных платежных систем будут стоять провайдеры и банки. Следовательно, электронные платежные системы выступают, с одной стороны, как составная часть банковской системы (и тогда на них распространяется действие банковского законодательства), а с другой – выступают самостоятельными субъектами, осуществляющими расчетные операции.

Платежная система *– это финансовая инфраструктура обеспечивающая совершение финансовых транзакций между банками и иными участниками рынка финансовых операций.*

С позиции технической составляющей – это аппаратно-программный комплекс со своей технической инфраструктурой, сводом правил и процедур, обеспечивающих бесперебойное совершение финансовых транзакций согласно международному, национальному законодательству и своим правилам.

Типичная платежная система может состоять из следующих составляющих: организации (подразделения) осуществляющие платежи, программно-аппаратное обеспечение, осуществляющее внутренние и внешние финансовые транзакции и нормативная правовая база, регламентирующая работу. Ключевой задачей платежной системы является оперативное проведение взаиморасчетов между участниками.

Можно выделить такие виды платежных систем как: системы с участием наличных денег; безналичные платежные системы; банковские платежные карты; электронные платежные системы.

Платежная система может быть разного уровня: может работать как на уровне одной страны, так и обеспечивать интересы нескольких стран локальными (например, SEPA в Европе) или быть международной (например, SWIFT). В международных расчетах особое место занимает система международных межбанковских расчетов SWIFT (Society for Worldwide Interbank Financial Telecommunication – сообщество всемирных межбанковских финансовых телекоммуникаций), которая охватывает более 11000 банков во всем мире. В системе SWIFT каналы через которые проходят финансы являются инфраструктурными решениями, которые обеспечивают передвижение денежных средств от одного субъекта к другому, например, от покупателя продавцу. В отдельных случаях под международной платежной системой имеют ввиду только системы обслуживающие платежные карты (типа VISA, MasterCard и др.).

В Республике Беларусь наиболее распространенными электронными платежными системами являются:

Ю.Money (один из сервисов Яндекса). После регистрации в системе создается электронный кошелек, который пополняется с использованием банковской платежной карты или наличных денег. Используется для оплаты товаров и услуги посредством компьютерной сети Интернет, а также для

совершения денежных переводов. Предоставляется возможность выпуска виртуальной карты, которой возможна оплата товаров и услуг при онлайн-платежах, где принимают к оплате банковские платежные карты.

WebMoney. Система российского происхождения, имеющая электронные аналоги российского и белорусского рубля, украинской гривны, казастанского тенге, доллара США, евро, золота, криптовалют (биткоина, лайткоина), которая используется во многих странах СНГ. Является одним из популярных сервисов электронных кошельков. После регистрации выдается номер в системе, который называется WMID, имеется возможность создания электронных кошельков в нужной валюте, к которым возможен выпуск виртуальной карты.

PayPal. Международная мультивалютная платежная система, действующая во многих странах мира, которая используется для различных платежей. При регистрации указываются полные данные, в том числе адрес электронной почты, и открывается счет без присвоения номера, вместо него используется указанный при регистрации адрес электронной почты. Для проведения платежей необходима привязка платежной карты к счету на сайте.

Qiwi. Регистрация в системе происходит по номеру мобильного телефона, который является счетом в системе и пополняется, например, через платежный терминал банковской картой. Возможен выпуск виртуальной карты или платежной карты Visa.

В Республике Беларусь также функционируют национальные платежные системы:

IPay-сервис, интегрированный с названными выше платежными системами, а также с ЕРИП и мобильными операторами.

Также в Республике Беларусь Национальным банком создана система провайдер «Расчет» (Единое расчетное информационное пространство), с помощью которой осуществляется поддержка при проведении онлайн-платежей. ЕРИП позволяет проводить различные виды расчетов, включая коммунальные услуги, покупки в интернет-магазинах, билеты в кино и др. Возможно подключение системы ЕРИП как напрямую, так и с помощью платежных агрегаторов.

Платежный агрегатор *обрабатывает онлайн-платежи*. Так, например, владелец интернет-магазина либо самостоятельно организовывает прием платежей с каждой из платежных систем, либо заключает договор с платежным агрегатором, у которого имеются технические решения для работы с платежными системами.

Наиболее распространенными платежными агрегаторами в Республике Беларусь являются:

WebPay (обеспечивает комплексные решения для приема онлайн-платежей по картам Visa, MasterCard, Белкарт);

Платежный агрегатор bePaid предназначен для юридических лиц и индивидуальных предпринимателей, которые продают товары (услуги) через компьютерную сеть Интернет. Данная система принимает оплату с помощью карт Visa, MasterCard, Белкарт, Халва. Проводит платежи в белорусских и российских рублях, а также в евро и долларах.

Агрегатор Assist может принимать к оплате банковские карты Visa, MasterCard, Maestro, American Express, Белкарт прямо на сайте.

Агрегатор EasyPay позволяет осуществлять платежи банковскими картами Visa и MasterCard, а также через систему ЕРИП.

Одними из наиболее популярных платежных агрегаторов в Российской Федерации являются Яндекс.касса, Robokassa, Z-payment и другие.

Платежный шлюз *– это сервис, который осуществляет маршрутизацию платежа.* С технической точки зрения платежный шлюз является программным модулем, который распределяет (осуществляет маршрутизацию) платежа между участниками транзакции: интернет-магазин, банк и третьи стороны, вовлеченных в процесс (например, предоставляющие услуги эквайеринга).

Платежный шлюз является интегратором платежных решений, который не выполняет какой-либо расчетно-финансовой функции. Однако платежные агрегатор и шлюз осуществляют интеграцию платежных инструментов для осуществления онлайн-платежей посредством широкого набора разный опций (платежные карты, электронные кошельки, оффлайн-платежи и др.).

Отличия платежного агрегатора и платежного шлюза:

платежный агрегатор аккумулирует денежные средства клиента у себя, что делает его полноценной небанковской кредитной организацией;

платежный шлюз лишь маршрутизирует платеж, с денежными средствами, вовлеченными в транзакционный обмен, не взаимодействует. Другими словами, платежный шлюз исключительно выполняет роль технологического посредника;

платежный шлюз в отличии от платежного агрегатора не несет ответственности за транзакцию, соответственно не несет риски по движениям денежных средств (например, возвраты);

платежный агрегатора аккумулирует денежные средства клиентов на своем счете прежде чем отсылать их в банк. Из-за этого может возникать риск небольшой отсрочки платежа по отношению к банку, а также возможность создания прецедента с «заморозкой» денежных средств при технологических сбоях;

платежные шлюзы в основном предоставляют услуги мультиэквайринга, при возникновении проблем с обработкой платежа в одном банке, шлюз быстро перемаршрутизирует платеж в другой банк.

Таким образом, основное отличие заключается в том, что платежный шлюз является технологическим партнером, который маршрутизирует платеж, не взаимодействуя с денежными средствами клиентов, в то время как платежный агрегатор их аккумулирует у себя.

Банк-эквайер *– кредитно-финансовая организация, обеспечивающая расчеты по банковским платежным картам в торгово-сервисных организациях.* Для обработки онлайн-платежей банк-эквайер использует платежный агрегатор или платежный шлюз.

Эмиссионный банк *(или кредитно-финансовая организация) осуществляющая выпуск (эмиссию) и в отдельных случаях обслуживание платежных карт, являющаяся владельцем платежной карты.* Основные функции банка-эмитента следующие: открытие счета, выпуск платежной карты, проведение авторизации платежей по своим платежным картам, совершение платежа в сторону продавца, если клиент совершил покупку, обеспечение безопасности транзакций.

Процессинговый центр *– организация или его структурное подразделения, обеспечивающее технологическое и информационное взаимодействие между участниками расчетов.*

4.2. Глобальная сеть Интернет: структура, основные понятия и термины, необходимые в работе сотрудника правоохранительных органов

Интернет образует глобальное информационное пространство, служит физической основой для Всемирной паутины и множества других систем (протоколов) передачи данных. В настоящее время, когда употребляется термин «Интернет», чаще всего имеется в виду Всемирная паутина и доступная в ней информация, а не сама физическая сеть.

Интернет (англ. Internet) – всемирная система объединённых компьютерных сетей, построенная на использовании протокола IP и маршрутизации пакетов данных.

Консорциум Всемирной паутины (англ. World Wide Web Consortium, W3C) разрабатывает для Интернета единые принципы и стандарты (называемые «рекомендациями», W3C Recommendations), которые затем внедряются производителями программ и оборудования. Таким образом, достигается совместимость между программными продуктами и аппаратурой различных компаний, что делает Всемирную сеть более совершенной, универсальной и удобной. Все рекомендации консорциума Всемирной паутины открыты, то есть не защищены патентами и могут внедряться любым человеком без всяких финансовых отчислений консорциуму. С каждым годом количество пользователей сети Интернет растет, а размер данных в достигает 2.7 Зеттабайт (1 ЗБ ~ 1012ГБ), при этом ежегодно количество пользователей и устройств, подключенных к сети, увеличивается на 6% и 10% соответственно.

Сеть Интернет рассматривается в технологическом и социальном смысле как:

информационно-коммуникационное средство, обеспечивающее передачу, обработку и хранение информации (технологический подход) – представляют интерес технологические вопросы функционирования;

сложный социокультурный феномен, оказывающий влияние на многие стороны жизни общества и образующий особую среду реализации

определенных видов деятельности и проявления специфических общественных отношений (социальный подход).

Для обучения и описания схемы взаимодействия сетевых объектов с определением списка правил и задач предназначена ***модель OSI***. При этом современная сеть Интернет основана на более простой модели TCP/IP, однако 7-уровневая модель OSI используется, поскольку помогает визуализировать и показывать то, как работают компьютерные сети.

Уровни модель OSI:

прикладной,

презентационный,

сессионный,

транспортный,

сетевой,

канальный

физический.

На **физическом** уровне происходит передача физических сигналов от источника к получателю, обеспечивается кабельное или беспроводное соединение. Осуществляется оперирование такими категориями как кабель, беспроводная технология, кодирование единиц и нулей.

На **канальном** уровне обеспечивается доставка данных адресату и их целостность, устанавливается соединение между двумя физически связанными узлами в сети. Осуществляется адресация, и адресом является *MAC-адрес*, т. е. появляется первый идентификатор.

На **сетевом** уровне осуществляется маршрутизация и появляется такой идентификатор как *IP-адрес*. Также программное обеспечение этого уровня выполняет функции аутентификации и авторизации. Сетевой уровень использует сетевые адреса (обычно адреса интернет-протокола) для маршрутизации пакетов на конечный узел.

Транспортный уровень обеспечивает передачу данных по сети *TCP и UDP* (потоковое видео и игровая графика). Разница заключается в том, что различные транспортный протокол применяется для разных категорий трафика. На этом уровне появляются понятия портов.

Протоколы, описанные на следующих уровнях, работают одновременно на нескольких уровнях модели OSI, поэтому нет четкого разделения на сеансовый и презентационный уровни. В связи с этим в настоящее время основным используемым стеком является TCP/IP.

На сессионном уровне обеспечивается виртуальное соединение между приложениями, поддержка сеанса или сессии связи. Другими словами, на этом уровне обеспечивается связь между приложениями и доставка данных.

На **презентационном** уровне осуществляется преставление и преобразование форматов данных (например, GIF, JPEG, MPEG и др.).

Прикладной уровень используется конечными пользователями программного обеспечения, такими как веб-браузеры и почтовые клиенты. Обеспечивается реализации конкретных действий, например, получение html-кода или email-сообщения адресатом. Предоставляются протоколы, которые позволяют программному обеспечению отправлять и получать данные. Этот уровень также определяет протоколы для конечных приложений, такие как система доменных имен (DNS), протокол передачи гипертекста (HTTP), протокол доступа в Интернет (IMAP), протокол передачи файлов (FTP) и др.

Модель OSI и TCP/IP и являются концептуальными моделями, используемыми для описания всех сетевых коммуникаций, в то время как сама модель TCP/IP также является протоколом, используемым во всех операциях сети Интернет. Модель TCP/IP используется как для моделирования текущей архитектуры Интернета, так и для предоставления набора правил, которым следуют все формы передачи по сети. Можно рассматривать сеть Интернет и как совокупность сетей различного типа и физических устройств, объединенных протоколами семейства TCP/IP (TCP/IP – сетевая модель передачи данных, представленных в цифровом виде) для обмена и передачи информации между ними.

Уровни модель TCP/IP**:**

канальный,

межсетевой,

транспортный,

прикладной.

OSI	TCP/IP
прикладной	прикладной
презентационный	
сессионный	
транспортный	транспортный
сетевой	межсетевой
канальный	канальный
физический	

Поскольку процесс информационного обмена посредством сети Интернет обезличен, его источник может быть определен, например, по IP-адресу, т.е. по уникальному идентификатору компьютера, под которым он известен в сети. Ввиду ограниченного количества IP-адресов адресные пространства распределяются иерархическим способом.

Организации, управляющие адресным пространством.

ICANN (Internet Corporation for Assigned Names and Numbers) – корпорация по управлению доменными именами и IP-адресами – независимая международная некоммерческая организация для регулирования вопросов, отвечает за ведение записей выделенных и еще не выделенных блоков IPv4-адресов, IPv6-адресов. Также осуществляет выделение больших блоков IP-адресов пяти региональным интернет-регистратурам согласно глобальным политикам.

IANA (Internet Assigned Numbers Authority) – администрация адресного пространства Интернет управляет пространством IPv4-адресов, распределяет большие блоки адресов между пятью региональными реестрами. Координирует работы по выработке технических параметров протоколов; осуществляет административные функции по управлению корнем системы доменных имен; распределяет блоков IP-адресов и др.

RIR (Regional Internet Registry) – региональный Интернет регистратор. Организация, занимающаяся вопросами адресации и маршрутизации в сети Интернет.

American Registry for Internet Numbers(ARIN) – Северная Америка;

RIPE Network Coordination Centre (RIPE NCC) – Европа, Ближний Восток и Центральная Азия;

Asia-Pacific Network Information Centre (APNIC) – Азия и Тихоокеанский регион;

Latin American and Caribbean Network Information Centre (LACNIC) – Латинская Америка и Карибский регион;

African Network Information Centre (AfriNIC) – Африка.

LIR (Local Internet Registry) –локальный интернет-регистратор.

ISP (Internet Service Provider) – организация, предоставляющая пользователям доступ к сети Интернет и связанные с этим услуги.

Таким образом, IANA выделяет блоки адресного пространства региональным интернет-реестрам, они выделяют блоки IP-адресов локальным интернет-реестрам, которые, в свою очередь, распределяют эти адреса между конечными пользователями.

IP-адрес *(англ. Internet Protocol Address «адрес интернет-протокола») – уникальный сетевой адрес узла в компьютерной сети.*

Форматы IP-адреса:

IPv4 – 87.252.235.11.

IPv6 – 2001:0DB8::/32 или 2001:0db8:11a3:09d7:1f34:8a2e:07a0:765d.

В зависимости от цели, которую должны выполнять IP-адреса, их можно разделить на:

внутренний (локальный) и внешний;

статический и динамический.

Причем при построении компьютерных сетей не используются какие-то отдельные типы. То есть, не может быть просто локальный IP-адрес – он всегда либо локальный динамический, либо локальный статический.

Внешний («белый», публичный) *IP-адрес – это IP-адрес, который входит в диапазон IP-адресов, предназначенных для сети Интернет (те диапазоны, которые не относятся к локальным).*

Внутренний («серый», частный, внутрисетевой, локальный) *IP-адрес – IP-адрес внутри частной сети провайдера или домашней сети, это адреса узлов, которые не требуют доступа в сеть Интернет.*

Статический *IP-адрес (постоянный, неизменяемый) закрепляется за устройством на постоянной основе, он не может быть присвоен никакому другому компьютеру.*

IP-адрес называют ***динамическим*** *(непостоянным, изменяемым), если он назначается автоматически при подключении устройства к сети и используется в течение ограниченного промежутка времени, указанного в сервисе назначавшего IP-адрес.*

Несмотря на иерархичность и кажущуюся прозрачность системы распределения IP-адресов, при идентификации конечного пользователя имеется ряд особенностей. В последние годы популярными интернет-провайдерами становятся операторы сотовой связи. Общее количество IP-адресов не увеличится, поэтому всегда используется комбинация из частных и публичных адресов. Из-за недостатка свободных IP-адресов используется технология NAT (англ. Network Address Translation – преобразование сетевых адресов).

Технология NAT *(преобразование сетевых адресов) – это технология, позволяющая разместить целую сеть (или сети) за одним IP-адресом, т.е. в одно и то же время определенный динамический IP-адрес присваивается большому количеству абонентов.*

Другими словами, эта технология позволяет раздавать пользователям «внутренние» адреса, а для того чтобы пользователи могли попасть в сеть Интернет, их запросы транслируются через внешний адрес. Осуществляется преобразование IP-адресов в сетевых пакетах, обычно в пакете указывается IP-адрес откуда пакет отправлен и IP-адрес куда пакет направляется. NAT позволяет динамически менять эти адреса и сохранять таблицу подменённых IP-адресов. Соответственно, для идентификации конечного пользователя необходимо знать IP-адрес интернет-ресурса, на который обращался устанавливаемый абонент, время обращения и другие сведения. Данное обстоятельство часто влечет за собой направление запросов, в том числе международных.

Согласно законодательству, **провайдеры и операторы сотовой связи обязаны осуществлять**:

идентификацию абонентских устройств при оказании интернет-услуг,

учет и хранение сведений об абонентских устройствах, а также сведений об оказанных интернет-услугах.

Помимо истории посещений пользователей провайдеры обязаны хранить:

MAC-адреса или идентификационные номера устройств, с которых пользователи выходят в интернет,

даты,

время начала/окончания соединений,

IP-адреса пользователей;

IP-адреса посещаемых ресурсов,

объем переданных и принятых данных.

Провайдер должен знать фамилию, имя, отчество, адрес, паспортные данные пользователей – физических лиц и индивидуальных предпринимателей.

Законодательно установлена обязанность осуществления идентификации пользователей интернет-услуг в интернет-кафе и интернет-клубах. Также собственники пунктов коллективного пользования интернет-услугами обязаны вести учет и хранение персональных данных пользователей интернет-услуг, сведений об интернет-услугах, которые были оказаны каждому конкретному клиенту. Хранение данных сведений должно осуществляться в течение года с момента оказания интернет-услуг.

Факт соединения и дальнейшие действия пользователя фиксируются аппаратурой провайдера и сохраняются в электронном журнале.

Кроме IP-адреса сетевой интерфейс имеет и другую важную характеристику – физический адрес (MAC-адрес).

MAC-адрес *(media access control address) – это уникальный идентификатор, присваиваемый каждой единице оборудования компьютерных сетей, т.е. идентификатор сетевой карты (интерфейса) или беспроводного адаптера.*

Форма представления MAC-адреса – «00:2B:67:56:76:15».

Этот адрес различен для разных сетевых адаптеров. Так, например, в большинстве своем ноутбуки оснащены:

адаптером LAN, для проводного подключения к специальному сетевому коммутатору или другому устройству;

адаптером WiFi, для беспроводного подключения к сети и/или другой компьютерной техники;

адаптером Bluetooth, обычно для беспроводного подключения к мобильным устройствам, реже для подключения к компьютерам и ноутбукам, из-за небольшой дальности и скорости подключения.

Стандартами предусмотрено использование уникального значения физического адреса, что осуществляется за счет обращения производителей сетевых карт к контролирующему органу (именуемому IEEE Registration Authority), выделяющему пул адресов для присвоения оборудованию. На основе известного MAC-адреса устройства можно в дальнейшем связать конкретное лицо непосредственно с фактом совершения противоправных действий. Получение этих сведений возможно, например, с помощью запроса сведений у провайдера. Также существуют интернет-сервисы, позволяющие определять производителя оборудования по известному MAC-адресу.

Доменное имя *– символьное имя, служащее для идентификации областей (единиц административной автономии в сети Интернет) в составе вышестоящей по иерархии такой области.* Каждая из таких областей называется доменом.

Общее пространство имён Интернета функционирует благодаря DNS – системе доменных имён. Доменные имена дают возможность адресации интернет-узлов и расположенных на них сетевых ресурсов (веб-сайтов, серверов электронной почты, других служб) в удобной для человека форме.

Домены разграничивают по трем уровням. Все домены первых двух уровней, в свою очередь, делятся на несколько групп по территориальной принадлежности или «отраслевому» назначению.

Домены высшего уровня. Имена с территориальной принадлежностью присвоены определенным странам. Так, к примеру, регистрация домена в

Республике Беларусь – .by (.бел), в России – .ru (.рф), в Украине – .ua, в США – .us. Благодаря этому можно определить государственную принадлежность того или иного сайта.

Группа доменов с определенным «отраслевым» назначением присваивается коммерческим организациям, информационным сайтам, провайдерам и сетевым организациям, телевизионным компаниям. К примеру, сайты коммерческих организаций используют – .com, для правительственных учреждений – .gov, некоммерческие организации – .org.

По указанным именам возможно определить конкретную направленность сайтов, но в последнее время хаотичное использование имен не всегда придерживается своего назначения. Списки территориальных и целевых доменов расположены на сайтах в сети Интернет, на сайтах регистраторов таких имен.

Домены первого уровня использовать как адрес своего сайта нельзя – они нужны для создания следующего уровня доменов, на базе любого из имен первого уровня возможно создание и регистрация доменов второго уровня и так по нарастающей. Имена второго уровня состоят из нескольких элементов и выглядят так: www.имя_сайта.доменное имя первого уровня. Пример доменов второго уровня: www. afisha.by, www.kino.ru.

Третий уровень создается, соответственно, на основе второго, и такие домены имеют вид, например, www.forum.kino.ru. Если при создании сайта провели регистрацию домена второго уровня, то каждый может вполне самостоятельно создать на его базе любое количество имен третьего. Соответствующая регистрация доменного имени для сайта может проводиться на специальных сервисах.

Информация о домене или об IP-адресе.

WHOIS *(англ. «Who is?» – «Кто такой?») – протокол, обеспечивающий предоставление информации о доменном имени или об IP-адресе.*

«Whois Service», представляющий собой сервис, для проверки доменов, позволяющий получить регистрационные данные о владельцах доменных имен, IP– адресов и автономных систем. Если доменное имя занято, можно узнать, кто его владелец и как с ним связаться. С помощью WHOIS можно установить

контактные данные владельца домена, дату создания, дату окончания регистрации и многое другое. Вся эта информация является публичной, однако некоторые регистраторы позволяют скрывать прямые контакты владельца домена, указывая контакты компании-регистратора.

Возможно направление запрос в компанию, которой делегирован IP – адрес (по данным «Whois»), для предоставления сведений об абоненте, который работал в сети Интернет, в интересующее нас время.

Как и с традиционными преступлениями, лица, совершающие киберпреступления, различными способами стараются скрыть все следы своей преступной деятельности.

Определенные трудности в процессе раскрытия преступлений возникают при использовании виновным различных технологических возможностей изменения или сокрытия IP-адресов, здесь в первую очередь речь идет о различных анонимайзерах и др. Не останавливаясь на технических аспектах работы указанных систем, следует отметить их сущность – все они могут обеспечить определенную анонимность доступа к различным интернет-ресурсам. Например, могут скрывать сведения об источнике запроса или пользователе либо передавать целевому серверу ложную информацию о нем.

К средствам анонимизации стоит отнести: прокси-серверы; VPN-сервисы; SSH-тунели; Dedicated-серверы; Tor; I2P серверы .

Прокси-сервер *– промежуточный сервер в компьютерных сетях, выполняющий роль посредника между пользователем и целевым сервером, позволяющий клиентам как выполнять косвенные запросы (принимая и передавая их через прокси-сервер) к другим сетевым службам, так и получать ответы.*

Прокси-сервер представляет собой физический или виртуальный сервер посредник, через который позволяет клиенту пропускать пакеты трафика через него, а также направлять запросы к сторонним ресурсам сети Интернет и получать от них ответы.

Изначально данная технология была создана для обеспечения безопасности сетевого оборудования клиента и обеспечения большей скорости

передачи пакетов из глобальной сети Интернет клиенту. Помимо этого, IP-адрес, который будет отображаться на ресурсе, расположенном в сети Интернет, не будет соответствовать адресу клиента, на ресурсе отобразится адрес непосредственно прокси-сервера, следовательно, установить какой пользователь осуществил запрос не представляется возможным без доступа к самому прокси-серверу, это и позволяет обеспечить некоторую анонимность клиента. Данный способ анонимизации довольно распространен ввиду того, что прокси-сервера используются повсеместно в компьютерных сетях и не требует особых познаний для использования.

VPN (виртуальная частная сеть) *представляет собой технологию, позволяющую произвести развертывание защищенной локальной сети поверх другой общедоступной сети, зачастую в качестве общедоступной используют глобальную сеть Интернет.*

Проходя авторизацию и подключаясь к VPN-сервису, пользователь пропускает свой трафик через данную сеть где данные подвергаются криптографической защите и степень доверия к этим сетям уже не играет большой роли, в результате клиент получает защищенное анонимизированное соединение с сетью Интернет. Сегодня существует множество различных VPN-сервисов, которые оказывают данные услуги на возмездной основе, что привело к развитию данной технологии и сокращению количества сбоев в ее работе.

Следующее средство анонимизации предназначено скорее для сокрытия данных передаваемых посредством сети Интернет, речь идет о ***SSH-туннелировании*** *представляющим собой способ передачи данных от одного узла к другому, когда заранее известен IP-адрес узла получателя, так же данный способ передачи данных шифрует данные пакетов протокола TCP/IP и работает зачастую именно с пакетами данного протокола.* То есть, имея такое соединение, два узла глобальной сети Интернет могут обмениваться информацией без посредников в виде каких-либо почтовых сервисов или социальных сетей и мессенджеров.

Использование **выделенных серверов** представляет собой предоставление в аренду провайдером реального физического сервера, на

котором возможно хранение, размещение информации и осуществление выхода в сеть Интернет. Интерес к данной технологии обусловлен тем, что данные серверы могут располагаться на территории иностранных государств, что взывает дополнительные сложности с получением информации об арендаторе сервера. Так же данная услуга позволяет арендатору осуществлять любую деятельность с использование данного сервера и устанавливать любые настройки и оперативные системы, при этом данные действия зачастую можно осуществлять удаленно.

Отдельное внимание стоит уделить ***сети «Tor»*** *(даркнет, «темный Интернет») – компьютерной сети, построенной с использованием технологии «луковичной» адресации, которая представляет собой передачу многократно зашифрованных пакетов данных, передаваемых посредством протокола TCP/IP, при этом передача осуществляется через несколько узлов сети и на каждом узле происходит расшифровка одного слоя шифрования.*

Основная идея заключается в том, что передача от узла к узлу происходит совершенно непредсказуемо и промежуточные узлы при расшифровке своего слоя получают лишь адрес следующего узла, информацией о содержании пакета, отправителе и получателе промежуточные узлы не обладают. Таким образом, выстраивается анонимизированная сеть для обмена данными. С использование Tor-браузера осуществляется вход в сеть «Tor».

Развитие данной технологии в русскоязычном регионе началось примерно в 2012 году, когда появилась стабильная версия Tor-браузера, появились русскоязычные сайты и данная технология начала набирать всеобщую популярность.

Все сервисы сети «Tor», работающие с использованием луковичной адресации, находятся в псевдодоменном пространстве «.onion», например:

«http://haystak5njsmn2hqkeweaxetahtwhsbsa64jom2k22z5afxhnpxfid.onion»,

«http://eludemailxhnqzfmxehy3bk5guyhlxnyhkcksv4gvx6d3wcf6smad.onion».

Сегодня пространство сети «Tor» насыщенно разнообразным контентом, в том числе и преступного характера, например, существуют площадки для

размещения объявлений о продаже товаров, ограниченных и запрещенных к обороту законом: торговля оружием, наркотиками, поддельными денег, хакерские услуги, вредоносное программное обеспечение и др. Помимо этого, осуществляется торговля конфиденциальной информацией, такой как данные граждан, сведения из государственных баз и банков данных, реквизиты банковских платежных карт и др.

Другое средство анонимизации схожее с Tor является I2P-сеть и сервисы, использующие её. ***Технология I2P*** *подразумевает организацию распределенной сети, особенность которой заключается в повсеместном использовании различных алгоритмов шифрования, в том числе и сквозного, что позволяет обеспечить ее анонимность.*

На текущем этапе данная технология не так распространена как Tor, она позволяет осуществлять доступ к скрытым ресурсам сети «Tor», при этом на большей скорости, еще одним преимуществом данной технологии и опасностью с точки зрения криминогенной обстановки в мире является возможность передачи потоковых данных, то есть появляется возможность использования: IP-телефонии, видеоконференций и других функций, требующих обеспечения потоковой передачи данных, что явно открывает новые возможности для преступников. Также, в отличии от сети Tor I2P, не осуществляет сбора статистики и все IP-адреса серверов являются анонимными, а сервисы данной сети расположены в псевдодоменном пространстве «.i2p».

4.3. Основы поисковой деятельности в сети Интернет при решении служебных задач

Интернет, представляя собой глобальную сеть обмена информацией, дает возможность в реальном времени изучать интересующего человека, следить за течением тех или иных социальных и экономических процессов, устанавливать данные юридических лиц. Но реализация данных возможностей требует грамотной реализации самого поиска информации в массиве неструктурированной информации.

Для успешного осуществления поисковой деятельности в сети Интернет для решения служебных задач необходимо обладать определенным уровнем технической подготовки и знаний в области субкультуры киберпреступности, в том числе взгляды и особенности общения киберпреступников. Стоит учитывать, что поиск информации в сети Интернет сам по себе в большинстве случаев не позволяет установить признаки преступлений, но способствует установлению фактов и следов прямо или косвенно указывающих на них.

Развитие социальных сетей и мессенджеров в настоящее время носит взрывной характер. Они все в большей степени оказывают влияние не только на повседневную жизнь, но и на политику, социальную сферу, и на сам характер общения между людьми. В Республике Беларусь среди социальных сетей на первом месте «ВКонтакте», «Одноклассники», также присутствуют «Instagram» «Facebook» и др.; самыми распространенными мессенджерами являются Viber, Telegram, WhatsApp. Данный феномен не просто вторгается в повседневную жизнь, социальные сети и мессенджеры в какой-то степени формируют общественное мнение.

Указанное позволяет рассматривать глобальные информационные сети в качестве особой среды для поиска общедоступной информации, в том числе содержащей признаки противоправной деятельности.

Процесс поиска в Интернете объектов или сведений об объектах заинтересованности, как правило, определяется в рамках изучения медиапространства, включающего в себя многочисленные интернет-ресурсы,

позволяющие, во-первых, создавать публичный или анонимный профиль в пределах определенной системы; во-вторых, выстраивать список контактов, с которыми они имеют связь; в-третьих, просматривать социальные связи, созданные другими в рамках системы.

Для решения служебных задач могут представлять интерес:

блог (микроблог) – веб-сайт, основное содержание которого составляет регулярно добавляемая текстовая или мультимедийная информация (LiveJournal, Blogger, Twitter, Qaiku и др.);

виртуальные службы знакомств – интернет-сервисы, предоставляющие пользователям Интернета услуги по виртуальному общению с другими пользователями, аналог реальных служб знакомств (LovePlanet.ru, Mamba, Tabor и др.);

мессенджеры – веб-ресурсы, предполагающие моментальный, в реальном времени обмен информацией (Viber, WhatsApp, Telegram, VIPole, Signal и др.);

сервисы объявлений, позволяющие публиковать объявления самого различного характера, а также искать необходимые товары, услуги и прочее посредством поисковых систем на данных сервисах;

сетевые и онлайн-игры – компьютерные игры, использующие постоянное соединение с сетью Интернет (Second Life, World of Worcraft, World of Tanks, War Thunder и др.);

службы обмена данными – сервисы, предоставляющие пользователям услуги хранения, доставки и показа видео, фото, музыки (YouTube, Instagram, MySpace Music, Flickr, Picasa и др.);

социальные сети, предоставляющие возможность организации взаимоотношений между различными субъектами социума;

электронная почта – служба по пересылке сообщений, предоставляющая возможность хранения больших массивов информации, иногда выделяя под контент некоторый объем облачных хранилищ (Gmail, Yandex, Mail.ru и т.д.).

Также на сегодняшний день практически каждый субъект, осуществляющий финансово-хозяйственную деятельность, имеет свой

представительский информационный ресурс в сети Интернет – **официальный сайт** (веб-сайт). Как правило, на таком сайте размещаются общие сведения, отображающие вид деятельности, режим работы, осуществляемые административные процедуры, состав руководства, структуру субъекта, проводимые закупки и конкурсы, различного рода документы, объявления, отчеты, фото, видео и т.д.

Организация поисковых действий в Интернете, как правило, должна основываться на определенной методике с использованием соответствующих информационных ресурсов и специальных программных средств, способствующих оптимизации временных затрат.

Все методологии сбора информации имеют определённые ограничения, основными проблемными аспектами являются:

большой объем данных приводит к появлению огромного количества сведений, которые необходимо проанализировать, чтобы оценить их полезность для решения поставленной задачи. Для этой цели существуют автоматизированные инструменты для фильтрации полученных данных (в том числе с использованием методов искусственного интеллекта). Однако огромный объем первичных, «сырых» данных, которые требуется обработать, остается проблемой при осуществлении поиска по открытым источникам;

трудоёмкость и потребность в квалифицированных аналитиках. Необходимо просматривать результаты работы автоматизированных инструментов, чтобы знать, являются ли собранные данные надежными и заслуживающими доверия;

необходимо поддерживать актуальность данных, что увеличить их ценность при использовании. Большое количество источников исчезает из-за ужесточения норм компьютерной безопасности и конфиденциальности;

ограниченность функционала средств для поиска информации. В основном одной программы с открытым исходным кодом для поиска недостаточно, а также они не пригодны для масштабирования, в корпоративных же инструментах много ненастраиваемых компонентов. Для успешного поиска информации требуется знание различных инструментов и умение, поиска новых методов получения информации.

достоверность информации в сети Интернет. Ввиду общедоступности данной сети информация в ней публикуется различными людьми часто совершенно без подкрепления фактической информацией или авторитетными источниками. На основании этого под недостоверной информацией понимается такая информация, которая не соответствует действительности и содержит сведения о событиях, явлениях, которых не существовало или сведения о них вообще не соответствуют действительности, являются неполными или искаженными. Задача лица, осуществляющего поиск информации, в таких условиях, отсеять недостоверную информацию либо проверить информацию, вызывающую сомнения.

Поиск информации в сети Интернет обладает определенными преимуществами по отношению к традиционным способам получения информации. К таким преимуществам помимо оперативности и доступности можно отнести также широкие границы поиска, на текущем этапе развития человечества не один источник не дает такого объема информации как сеть Интернет, что позволяет вести комплексный поиск информации об интересующем объекте в различных сферах знания и направлениях.

Значимая информация может находиться в форме текстовых сообщений, графических, видео- и аудиофайлов, ссылок на противозаконные источники и т. д. Надо определиться и с возможными форматами файлов, в которых может содержаться требуемая информация. Это может быть html-страница, текстовый документ в форматах txt, rtf, doc или docx, документ pdf, электронная таблица в форматах ods, xls или xlsx, аудио в формате mp3, flash-ролик формата swf, видео в формате avi и т. д.

Чтобы спланировать поиск, следует прежде всего определить объект поиска, сформулировать какую информацию необходимо найти. Если однозначно ответить на этот вопрос не представляется возможным, то поиск следует разделить на задачи с разными объектами.

Таким образом, **планирование поиска** заключается в трёх аспектах:

конкретные задачи поиска,

поисковая среда,

инструментарий.

Базовым поисковым инструментом являются поисковые системы. ***Поисковая система*** *– это система, предназначенная для поиска информации в сети Интернет.*

В настоящее время поисковые системы обеспечивают наиболее полный охват сайтов в сети Интернет и быстрое обновление информации, по сравнению с другими сервисами. Но несмотря на функционал и продвинутость своих алгоритмов, поисковые системы остаются машинами, они действуют в соответствии с программами, которые в них заложены.

Наиболее распространенными поисковыми системами являются Google и «Яндекс», в которых поисковые алгоритмы отдают предпочтение русскоязычным сайтам, даже если запрос введён на другом языке. Важно учитывать, что различные поисковые системы обладают собственными особенностями. При этом каждая поисковая система обладает своей зоной покрытия по доменам. Например, российская поисковая система «Яндекс» прежде всего работает с русскоязычными сайтами в доменных зонах ru, su, by и др. Это означает что выполнение одних и тех же поисковых запросов может давать различный результат ввиду различий в списках страниц лидеров по данным запросам составляемых системой.

Также представляет интерес поисковая система DuckDuckGo. Кроме собственного робота поисковик использует результаты других источников: Yahoo, Bing, «Википедия». DuckDuckGo не собирает данных о пользователе, не хранит логи (нет истории поиска), использование файлов cookie максимально ограничено. Все крупные поисковые системы стараются персонализировать поисковую выдачу на основе данных о человеке и его устройстве (настройках), в результате чего пользователь видит только те результаты, которые согласуются с его предпочтениями или которые система сочтёт таковыми. DuckDuckGo формирует ответ на запрос независимо от прошлых поисковых запросов.

Рассматривая особенности поисковой системы «Яндекс» необходимо учитывать такую возможность как язык поисковых запросов (операторы поиска). Зачастую правильность построения запроса в значительной мере влияет на его успешность и высокую релевантность результатов. Современные

поисковые системы используют в запросах такие элементы как логические операторы, например: «И», «ИЛИ», «НЕ», «|», «~» и др.

В поисковой системе «Google» существуют аналогичные операторы, но с другими наименованиями «site:», «filetype:», «or, and, not» и др. Так, например, первый предназначен для осуществления поиска по уже известному сайту, адрес сайта указывается после двоеточия, а текст запроса после адреса. Второй – для поиска по документам, тип которого указывается после двоеточия и текст самого запроса аналогично первому запросу.

Все возможности языка запросов поисковых систем обширны, рассматривать их все не представляется целесообразным, необходимую информацию можно получить на сайтах поддержки данных продуктов. Применение таких операторов в ходе поисковой деятельности в сети Интернет позволит избежать низкой релевантности результатов запросов ввиду того, что, например, преступники для обозначения тех или иных явлений, событий, сайтов, или действий могут использовать сленг.

Также одним из наиболее распространенных элементов повышения релевантности запросов является расширенный поиск (заполнение поисковой формы) и тематически фильтры поисковых систем. Например, поисковая система «Google» обладает такими поисковыми фильтрами как поиск картинок по тематике «Картинки», поиск местонахождения – «Карты». Данные фильтры позволяют исключить из результатов запроса часть сайтов, не подходящих по тематике, и сузить круг поиска информации.

Поисковые системы обладают обширным инструментарием в сфере поиска информации ввиду того, что поиск информации для пользователя их основная задача. При этом использование различных возможностей данных систем дают хорошие результаты, а их комплексное использование в разы повышает эффективность данной деятельности. При этом необходимо помнить, что алгоритмы работы поисковых систем различаются. Помимо этого, результат их работы представляет огромные объемы информации, которые необходимо анализировать вручную.

Касаясь специализированных программных продуктов поиска информации в сети Интернет, необходимо отметить что их особенность

заключается в том, что они работают с определенными средами нахождения информации или отдельными видами информации. Специализированные программные средства поиска информации в сети Интернет обладают различными специфичными свойствами, такими как среда поиска, тип данных, используемый как исходный для поиска и другое, что существенно снижает их универсальность. Такой подход позволяет увеличить эффективность осуществления поиска информации за счёт отсечения информации, не представляющей интереса.

Специалистами в данном направлении[10], как правило, **выделяются следующие направления поиска:**

по социальным сетям;

по никнейму (имени),

по фотографии;

поиск в сети Tor;

поиск криптовалютных кошельков и адресов.

Также в отдельных случаях может собираться информация о юридических лицах: о DNS-именах, IP-адресах, доменах и субдоменах, зарегистрированных за компанией, фактах компрометации почтовых адресов и др. Для решения данной задачи возможно использование онлайн-сервисов, обобщенной базой которых является Интернет-сервис «osintframework», который собрал и отсортировал по разделам различные инструменты и ссылки на них в сети Интернет.

Отдельной формой получения информации в сети Интернет можно считать мониторинг закрытых для общего доступа мест общения определенной направленности, что предполагает постоянное изучение сообщений, публикуемых в соответствующих чатах, форумах. В подобных местах могут появляться индикаторы, сигнализирующие о криминальной активности конкретных субъектов и др.

При осуществлении поиска информации о физическом лице первоначально необходимо осуществить проверку с помощью поисковых

[10] OSINT (Open source intelligence) – поиск на основе открытых источников, то есть набор из разных инструментов, которые позволяют нам эффективно искать, собирать и анализировать информацию из открытых источников сети Интернет.

систем используя фильтры и операторы, расширенный поиск, используя выборку по различной имеющейся информации (например, телефон, никнейм, фото, электронная почта или логин Skype), чтобы получить максимальное количество информации. Находя определённые данные необходимо их конкретизировать или дополнять существующий запрос, что обусловливает возможность получения новой информации.

Особенности поиска по социальным сетям.

Социальная сеть *– Интернет-платформа, которая используется для общения, знакомств, создания социальных отношений между людьми, которые имеют схожие интересы или офлайн (онлайн)-связи, а также для развлечения (музыка, фильмы) и работы.* Присутствует тенденция дублирования всех процессов из реальной жизни в виртуальную среду.

На сегодняшний день большинство пользователей сети Интернет имеют аккаунты в различных социальных сетях, при этом почти каждая социальная сеть представляет собой определенный объем информации о лице, создавшем там свою учетную запись. Отличительной чертой этих сетей является возможность объединения пользователей в группы, а также выделение одним пользователем сети других пользователей в качестве своих друзей. Существует большое количество как открытых, так и закрытых социальных сетей, объединяющих людей по широкому кругу интересов.Структурно социальные сети состоят из личных страниц пользователей и их сообществ. Как правило, в профиле указаны анкетные данные конкретного пользователя, а в сообществе – его любимые темы. Данное обстоятельство позволяет осуществлять анализ страниц пользователей и конкретных сообществ с целью поиска необходимой информации.

Для первоначального поиска по социальным сетям не требуется регистрация в них, так как поисковые системы группируют профили, принадлежащие одному и тому же человеку, если не установлены соответствующие ограничения в настройках.

Многие современные социальные сети обладают собственными системами поиска информации. Так, поиск может осуществляться непосредственно на сайтах социальных сетей по имеющейся информации (имя

и фамилия, никнейм), для конкретизации поиска используется фильтрация по региону, возрасту и другим параметрам. Например, социальная сеть «ВКонтакте» имеет свои поисковые операторы, позволяющие осуществлять его более эффективно. Одним из таких является оператор «near:», позволяющий осуществлять поиск фотографий рядом с координатами долготы и широты, указанным в запросе после символа двоеточия, позволяет просмотреть присутствие определенных лиц в указанном месте, если они делали фото. Операторы «type:reply» и «type:copy» позволяют искать необходимую информацию в комментариях и репостах. В целях поиска записей, содержащих ссылки на сайты или домены, используются операторы: «url:» и «domain:».

В случае, когда известен мобильный номер или адрес электронной почты, то возможно использование его на странице восстановления доступа к аккаунту для установления принадлежности определенного аккаунта или некоторых сведений о нем. Такая возможность предусмотрена также для мессенджеров и сервисов электронной почты.

Для осуществления поиска по социальным сетям существуют Интернет-сервисы, находящиеся в открытом доступе. Например, сервис *«Searchlikes»* (http://searchlikes.ru) позволяет проводить анализ страниц друзей конкретного пользователя с целью выявления их активности в сети Интернет, устанавливать и анализировать проставление «лайков», отметок «нравится» в социальной сети «ВКонтакте», а также выявлять комментарии пользователя как в Интернет сообществах (группах), так и на страницах других пользователей социальной сети.

Сервис поиска общих друзей и подписок *«220vk»* (https://220vk.com) предоставляет возможности по анализу аккаунтов социальной сети «ВКонтакте», в том числе устанавливать связи между людьми в социальной сети «ВКонтакте», взаимосвязи различных лиц (используя ID пользователей). Функция «онлайн-трекер» позволяет анализировать информацию о нахождении пользователя в социальной сети, показывая программный способ нахождения пользователя в сети (мобильная или десктопная версия).

«*Yasiv*» (https://www.yasiv.com) – сервис для анализа страниц социальных сетей и поиска взаимосвязей с использованием метода графов.

На данный момент актуальными являются telegram-боты, например:

VKHistoryRobot (@VKHistoryRobot) – бот в мессенджере «Telegram», который осуществляет доступ к историю профиля социальной сети ВКонтакте.

«Insight» (@ibhld_bot) – позволяет узнать, чем интересуется пользователь в мессенджере «Telegram», а также в каких группах состоит.

Особенности поиска по никнейму.

Никнейм (ник, имя) *– это псевдоним в сети Интернет (мессенджере). Никнеймы могут создаваться на основе искаженных имени и фамилии (например, oleg01_bondar), либо использоваться прозвища из игр и фильмов (например, terminator007), увлечений (например, football_player_1), реже создаются на основе реальных имени и фамилии.*

Для осуществления поиска по никнейму существует сервисы, находящиеся в открытом доступе, например:

namechk.com – это сервис, сканирующий большинство самых популярных интернет-ресурсов (социальных сетей) и отображающий ссылки на все аккаунты с интересующим никнеймом;

pipl.com – сервис, позволяющий искать пользователей не только по никнейму, но и по имени и фамилии;

where-you.com – сервис для поиска пользователей в социальных сетях, который позволяет найти человека по дате рождения и городу, указанному при регистрации;

www.user-searcher.com/ - сервис по поиску никнеймов на более чем 2000 сайтах.

checkuser.org – сервис осуществляющий поиск в различных виртуальных сервисах аккаунтов пользователей, работает на принципе поиска ключевого слова или схожих с ним слов, при этом это слово не обязательно должно иметь смысловую нагрузку, даже если для никнейма используется набор букв проверяется существование аккаунта в базе данных сервиса.

Также представляет интерес такое программное обеспечение как *«Snoop Project»*, возможности которого ограничиваются не только поиском по никнейму, а также осуществляется поиск по email-адресу (на каких интернет-ресурсах указан при регистрации адрес).

Особенности осуществления поиска по фотографии.

Выделяется несколько направлений поиска по фотографии:

установление личных данных человека по опубликованной (имеющейся) фотографии;

определение места снимка или загрузки фотографии и других данных.

В большинстве случаев возможности поиска по фотографии используются для установления профилей в социальных сетях, однако имеется возможность находить изображения и в других источниках, например, для поиска интересующих предметов и изделий. Результатом такого поиска станут Интернет-ресурсы, на которых распространяется или рекламируется данная продукция.

Могут представлять интерес следующие программные продукты и интернет-ресурсы для поиска по фотографии.

«*Findclone*» является аналогом «Findface», позволяющим найти по фотографии аккаунт в социальной сети «ВКонтакте». При этом фото может не находиться в сети, система анализирует непосредственно изображение лица на картинке и проводит поиск по всем фотографиям находящимися в социальной сети. На фотографии может присутствовать несколько людей, и система проанализирует каждого присутствующего на изображении. Также особенностью является то, что сервис ведет историю запросов и возможен возврат к ранее выполненному запросу без повторения действий.

Представляет интерес сервис «*Photo-Map*» (http://photo-map.ru), который выполняет поиск фотографий, размещенных в социальной сети «ВКонтакте» и отображает фотографию и страницу пользователя социальной сети, который ее разместил на странице. При этом область поиска можно указывать с точностью до 10 метров, а информация о фото содержит ссылку на страницу пользователя, дату фотографии и непосредственно саму фотографию.

https://search4faces.com/ - сервис, который позволяет осуществлять поиск по фото в таких социальных сетях как ВКонтакте, Одноклассники и ТикТок.

https://vk.watch/ - сервис, который позволяет осуществлять поиск по фото в социальной сети ВКонтакте.

«AVinfoBot» – бот в мессенджере «Telegram», который также позволяет осуществлять поиск по фото.

«EYE OF GOD» (@g5kfv6s3127x_cheke_bot) – бот в мессенджере «Telegram», сервис автоматического поиска информации в сети Интернет, в том числе по фотоснимкам.

«usersbox» (@UsersSearchBot) – бот в мессенджере «Telegram», сервис автоматического поиска информации в сети Интернет.

Необходимо отметить, что каждая цифровая фотография имеет свои метаданные, которые могут включать различные данные, в том числе о местоположении устройства в момент создания или распространения фотографии. Любой тип файла имеет свой стандарт метаданных, наиболее широкое среди которых имеет стандарт EXIF, являющийся неотъемлемой частью цифрового изображения. В настоящее время большинство ресурсов (социальных сетей и др.) шифрует метаданные, но если фотография передается без зашифровки, то появляется возможность установить: версию программного обеспечения устройства; дату, время в отдельных случаях место съемки; различные настройки устройства (баланс, ретуширование, выдержку, яркость). Сервисы для просмотра метаданных: средства операционной системы, графические редакторы (например, в *Photoshop* – File → File Info); программа *«ExifTool»* (https://exiftool.org); интернет-ресурс *http://exif.regex.info/exif.cgi*.

В свою очередь метаданные содержат не только цифровые изображения, но и практически любой файл. Таким образом, метаданные могут быть дополнительным источником информации.

Особенности осуществления поисковой деятельности в сети Tor. Для осуществления поисковой деятельности представляют интерес интернет-ресурсы, являющиеся поисковыми системами, работающими после входа с использованием браузера Tor, например, not Evil, LOOK, TORCH (один из самых старых поисковиков в сети Tor) и другие. При осуществлении поисковой деятельности необходимо учитывать, что сайты часто меняют адреса, загрузка данных происходит медленнее и поиск в связи с техническими особенностями функционирования сети в определенной степени органичен. Для осуществления поисковой деятельности необходимо знать адрес конкретного

ресурса, форума, которые можно найти с помощью поисковых систем либо на соответствующих форумах, телеграмм-каналах.

Особенности поисковой деятельности по криптокошелькам и криптоадресам. В настоящее время существует большое количество криптовалют, наиболее распространенной из них является Bitcoin и Ethereum. Криптовалюта представляет собой виртуальные цифровые активы, которые хранятся на криптовалютных-адресах в криптовалютных-кошельках. Все транзакции, перемещающие криптовалюты с одного адреса на другой, подписываются электронным образом и размещаются в сеть. Сведения о транзакции знает не только покупатель и продавец, все транзакции распространяются по всей сети, для обеспечения осведомленности каждого участника. Адрес принадлежит определенному кошельку, в котором может быть несколько адресов. В случае, когда в одном кошельке есть несколько адресов, то владелец у этих адресов один и тот же. Обнаружение такого кошелька может быть полезно тем, что появится возможность установить неизвестные адреса того же субъекта. Также необходимо учитывать, что существуют криптообменники и адрес с сотнями тысяч транзакций, вероятнее всего, принадлежит такому обменнику.

Задачи **поисковой деятельности в данном направлении***:*

идентификация интересуемого лица;

обнаружение криптовалюты (похищенной, использованной в преступной деятельности).

Поиск в данном направлении состоит из нескольких этапов:

идентификация конкретной цели (адрес, кошелек);

поиск информации о «серых» (подозрительных) действиях цели в настоящее время и прошлом;

поиск людей и организаций, связанных с целью, для последующего установления.

Основные способы установление пользователя по криптоадресам и криптокошелькам:

во-первых, использование поисковых интернет-систем. Поиск может привести к Интернет-страницам с упоминанием адреса или кошелька. Отдельные из них могут быть связаны с блокчейн-обозревателями, которые не содержат деталей, приводящих к идентификации конкретного лица. Тем не менее, возможна ситуация беспечности лиц, представляющих интерес, когда публикуются криптоадреса и криптокошельки в сети Интернет с привязкой к конкретному лицу, объявлению, странице в социальной сети и др.;

во-вторых, поиск на «криптовалютны» онлайн-форумах (например, www.bitcointalk.org), где адреса могут содержаться в сообщениях, профилях участников и др. Отдельные форумы отображают общедоступную информацию о лице, который создал сообщение (например, никнейм, контактные данные и списки всех сообщений вместе с отметками времени);

в-третьих, для идентификации и поиска информации о криптокошельке можно воспользоваться соответствующими *операторами поисковой системой* «Google»: explorer, block, site.

Так, чтобы исключить из поисковой выдачи все обозреватели блокчейна используются запросы:

«34byG3bC77coRTYWJioxW5GVvAfLp9zL2K-**block**»

«3Jx1ThGhh5P9vL5XkMw1NauH2YEDSZo4Wd –**explorer**».

Для поиска сведений о криптокошельке на определенном –Интернет-ресурсе используется запрос:

«**site:**bitcointalk.org 34byG3bC77coRTYWJioxW5GVvAfLp9zL2K».

в-четвертых, использование блокчейн-обозревателей, представляющих собой поисковый Интернет-ресурс для поиска блоков блокчейна, позволяющие просматривать блоки, адреса кошельков, сведения о транзакциях и другую информацию в блокчейне. Для каждая криптовалюты реализован собственный блокчейн и обозреватель, который необходимо использовать для просмотра данных (Bitcoin, Ethereum, Litecoin и др.). Блокчейн является публичной базой данных, хранящая все данные в незашифрованном виде, однако блокчейн не хранится централизованно, а находится у тысячи частных пользователей и компаний, где работают криптоклиенты. Каждый пользователь может загрузить файлы в блокчейн и проанализировать данные, импортировать их в базу

данных или запросить их. Блокчейн-обозреватель используется для запроса блокчейна и отображения результатов. Необходимо учитывать, что идентификация интересуемых адресов (кошельков) не может быть реализована блокчейном, особенностью которого является поддержка кошелька (адреса) без каких-либо ссылок на пользователя. В этой связи необходим анализ информации, полученной из блокчейна со сведениями из других источников;

в-пятых, проверка адреса (кошелька) на Интернет-ресурсе Walletexplorer.com, осуществляющем установление отдельных сведений используемого кошелька (адреса), таких как криптообменник, провайдер кошелька, платежный процессор, игровой или торговый сайт. Также *Walletexplorer.com* в определенной степени позволяет узнать, к какому кошельку относится тот или иной адрес либо установить какие адреса содержит тот или иной кошелек. В свою очередь необходимо учитывать, что разработчики ресурса в настоящее время не производят его обновление;

в-*шестых, отдельно необходимо отметить инструмента анализа криптотранзакций* «*Crystal Block Explorer*» (https://explorer.crystalblockchain.com), позволяющий анализировать криптотранзакции и отлслеживать происхождение криптоактивов, а также имеется возможность визуализации криптотранзакций. С помощью указанного инструмента возможна проверка связи конкретных транзакций или активов с криптобиржей, криминальным Интернет-магазином и др.

Для анализа криптовалют (транзакций и определения владельцев адресов) возможно использование коммерческих инструментов, таких как Chainalysis, Elliptic, Blockseer, Ciphertrace, Bitanalysis и др. Указанные программные продукты обладают большим поисковым функционалом по поиску и анализу криптокошельков (адресов) и графической визуализацией связей между кошельками, также некоторые предоставляют дополнительную информацию, полученную из ресурсов сети Tor.

Представлять интерес следующие программные продукты и интернет-ресурсы для поисковой деятельности в данном направлении.

«*Ethtective*» (https://ethtective.com) – интернет-сервис позволяющий визуально отслеживать транзакции криптовалюты Ethereum.

Интрнет-сервисы, которые возможно использовать для выявления связи криптоактивов с биржами и др.: *https://bitinfocharts.com, https://oxt.me*.

Сервисы-отзывики, могущие содержать сведения о кошельках их владельцах, упоминания на интернет-ресурсах, причастных к правонарушениям: *https://www.bitcoinabuse.com, https://www.bitcoinwhoswho.com, https://checkbitcoinaddress.com, https://scam-alert.io, https://badbitcoin.org, https://cryptscam.com*.

В свою очередь необходимо учитывать, что в противоправной деятельности могут использоваться криптомиксеры, усложняющие отслеживание криптовалюты. Миксеры позволяют вносить криптовалюту, а затем смешивать ее с большим пулом «случайных» транзакций. Таким образом, исходная криптовалюта запутывается в большом количестве сумм из множества разных и неизвестных источников.

В свою очередь в настоящее время в поисковой деятельности представляет интерес интернет-мессенджер «Telegram», имеющий широкую функциональность для работы с ботами. Все они выполняют различные функции, это происходит за счет работы ботов с открытыми базами данных и телефонными справочниками. Применение подобных программ широко распространено, также созданы боты, которые служат для осуществления поисковой деятельности.

Преимущества ботов:

удобство, скорость получаемой анализируемой информации;

простота интерфейса, все в одном приложении «Telegram», как правило вводится номер (почта, ip-адрес и др.);

отсутствие регистрации на специализированных сайтах;

Telegram-боты, которые в настоящее время можно использовать в поисковой деятельности: @get_kontakt_bot, @mailsearchbot, @telesint_bot, @autotekarubot и др.

При осуществлении поисковой деятельности представляет интерес программное обеспечение для осуществления анализа информации. Одной из программ является «i2 Analyst's Notebook». Программное обеспечение предназначено для построения графовых схем для анализа, установления связей

и формирования аналитического отчета. Также позволяет создавать графики таймлайна для анализа событий и последовательности их изменения, позволяет анализировать социальные сети, мобильные переговоры, события, геоданные в разрезе времени и др.

Возможности «IBM Security i2 Analyst's Notebook»:

анализа связей, визуализация данных позволяет увидеть взаимоотношения между объектами (например, людьми или организациями);

хронологический анализ, отображение информации на временной шкале показывает, как разворачиваются цепочки событий в течение интересующих периодов;

анализ социальных сетей. Помогает оценивать и анализировать структуры групп и потоки обмена информацией в сетях и визуализировать информацию;

расширенная аналитика для быстрого нахождения неочевидные связей.

Также представляет интерес программное обеспечение «*Maltego*» являющееся инструментом для построения и анализа связей между различными субъектами и объектами. Особенностями являются: визуализирование полученных данных, поиск в сети Интернет на основе открытых Интернет-источников, автоматический анализ открытых источников и автоматическое построение взаимосвязей между обнаруженными объектами.

Программное обеспечение «Maltego» также позволяет:

получать сетевую и доменную информацию, такую как: доменные имена, whois информация, DNS записи, IP-адреса и др.;

искать информацию по адресу электронной почты, Интернет-ресурсу, группе в определенных социальных сетях и др.;

проверять адреса электронной почты;

извлекать метаданные из файлов на целевых доменах.

В заключении необходимо отметить, что при осуществлении поисковой деятельности в сети Интернет необходимо помнить, что весьма динамична как сама поисковая среда, так инструментарий, в том числе рассмотренный, что обусловливает необходимость постоянного обладания актуальной информацией.

ГЛАВА 5
КОМПЬЮТЕРНАЯ ИНФОРМАЦИЯ: ОБНАРУЖЕНИЕ И АНАЛИЗ

5.1. Понятие и классификация компьютерной информации

Анализ правоохранительной практики последнего десятилетия наглядно демонстрирует потребность деятельности по выявлению и раскрытию преступлений в эффективных уголовно-процессуальных рекомендациях, методиках борьбы как с «традиционными» преступлениями, так и с видами преступлений, где компьютерные технологии предоставляют широкие возможности совершенствования способов совершения преступлений, их механизмов.

Представляется, что разработка средств борьбы с киберпреступностью требует, прежде всего, методолого-теоретического осмысления проблемы и выявления сущности основных уголовно-процессуальных категорий применительно к рассматриваемой сфере деятельности. В уголовно-процессуальной среде одним из самых важных институтов является процесс доказывания. Структурным компонентом данного процесса выступает определение компьютерной информации.

Согласно ст. 18 УК Республики Беларусь под ***компьютерной информацией*** *понимается информация, хранящаяся в компьютерной системе, сети или на машинных носителях, обрабатываемая компьютерной системой либо передаваемая в пространстве с помощью любых программно-технических средств.*

Компьютерная информация может быть представлена в различных формах, таких как электронные письма, текстовые сообщения, сообщения в

социальных сетях, история просмотра интернет-страниц, цифровые изображения и видео, компьютерные файлы, данные GPS и метаданные[11].

Допустимость компьютерной информации зависит от различных факторов, таких как подлинность, надежность и целостность. Чтобы установить подлинность и надежность компьютерной информации, важно обеспечить их сбор, сохранение и анализ надлежащим и точным образом. Сбор компьютерной информации может быть сложным процессом, требующим специальных навыков и знаний, и должен осуществляться в соответствии с юридическими требованиями и руководящими принципами.

Одной из основных проблем при сборе компьютерной информации является обеспечение того, чтобы они не были подделаны или изменены в процессе сбора. Для решения этой задачи часто используются специальные инструменты и методы для получения и сохранения компьютерной информации. Это предполагает создание копии исходных данных, использование таких методов, как хэширование, для проверки целостности данных, а также соблюдение надлежащей цепочки хранения для обеспечения того, чтобы компьютерная информация не была изменена.

Помимо технических проблем, компьютерная информация также поднимает важные юридические и этические вопросы, такие как неприкосновенность частной жизни, конфиденциальность др. В некоторых случаях сбор компьютерной информации может быть связан с ограничением конституционных прав граждан, поэтому важно обеспечить, чтобы сбор и использование компьютерной информации осуществлялись с соблюдением соответствующих правовых норм.

Использование компьютерной информации становится все более важным в современном судопроизводстве и, вероятно, будет продолжать играть важную роль в системе правосудия. Поскольку технологии продолжают развиваться, для специалистов в области права важно быть в курсе последних событий в области информационных технологий и обладать необходимыми навыками и

[11] Метаданные - это данные о данных (об их составе, содержании, статусе, происхождении, местонахождении, качестве, форматах, объёме, условиях доступа, авторских правах и т. п.).

знаниями для эффективного сбора, сохранения и анализа компьютерной информации.

Компьютерная информация может быть классифицирована по обособленным критериям, в зависимости от различных факторов, таких как тип устройства, формат данных, источник и метод сбора.

По типу устройства:

информация на базе компьютера: компьютерные файлы, электронные письма, история посещенных интернет-ресурсов, журналы чатов, базы данных, системные журналы, записи в реестре и т.д.;

информация на базе мобильных устройств: текстовые сообщения, журналы вызовов, данные о местоположении, фото и видео, активность в социальных сетях и т.д.;

информация на основе устройств IoT[12]: данные с устройств, таких как интеллектуальные динамики, интеллектуальные термостаты, интеллектуальные приборы и носимые устройства.

В зависимости от формата данных:

структурированные данные: данные, хранящиеся в определенном формате, такие как базы данных, электронные таблицы и журналы;

неструктурированные данные: данные, которые не имеют фиксированного формата, например, электронные письма, сообщения в социальных сетях и журналы чатов.

В зависимости от источника данных:

волатильные данные: данные, которые существуют только в памяти или кэше[13] компьютера, такие как запущенные процессы, сетевые соединения и открытые файлы.

энергонезависимые данные: данные, которые хранятся на физическом устройстве, например, на жестких дисках, USB-накопителях и картах памяти.

По методу сбора:

[12] Интернет вещей (англ. internet of things, IoT) — концепция сети передачи данных между физическими объектами («вещами»), оснащёнными встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой.

[13] ***Кэш*** *– специальная область на диске или в операционной памяти компьютера, предназначенная для временного хранения информации и для часто используемых данных и команд.*

активный сбор: данные, получаемые непосредственно с устройства, например, при криминалистической визуализации или получении в реальном времени.

пассивный сбор: данные, полученные косвенным путем, например, анализ сетевого трафика[14] или записи с камер наблюдения.

Цифровые идентификаторы. Помимо классификации компьютерной информации дополнительно необходимо выделить цифровые идентификаторы устройств, на которых хранится или обрабатывается компьютерная информация, которые имеют значение при установлении лица, совершившего преступление.

Цифровые идентификаторы *– это уникальный код или значения, которые используются для идентификации цифровых объектов или субъектов, таких как веб-сайты, файлы, пользователи и устройства.*

Идентификаторы имеют решающее значение в цифровом мире, поскольку они помогают управлять, защищать и упорядочивать поток информации в различных системах и платформах.

Существуют различные цифровые идентификаторы, каждый из которых служит определенной цели.

Единый указатель ресурса (URL).

Единый указатель ресурса (URL) *– это уникальный идентификатор, который используется для поиска и доступа к веб-страницам и ресурсам в Интернете.*

Когда пользователь получает доступ к веб-сайту или ресурсу с помощью веб-браузера, браузер отправляет запрос на сервер, на котором размещен ресурс, а сервер отвечает, отправляя запрашиваемое содержимое обратно в браузер. Заголовки запроса и ответа содержат информацию о браузере пользователя, времени и дате запроса, а также другие метаданные, которые могут быть полезны при проведении осмотра компьютерной информации.

[14] ***Сетево́й тра́фик, или интерне́т-тра́фик*** *(англ. traffic — «движение», «грузооборот»), — объём информации, передаваемой через компьютерную сеть за определённый период времени. Количество трафика измеряется как в пакетах, так и в битах, байтах и их производных: килобайт (КБ), мегабайт (МБ) и т. д.*

URL состоит из нескольких компонентов, которые используются для идентификации и определения местонахождения определенного ресурса в Интернете, например, веб-страницы или файла.

Компоненты URL обычно включают:

Протокол. Протокол определяет метод, используемый для доступа к ресурсу, например HTTP, HTTPS, FTP или Telnet.

*Домен***.** Домен (также известный как имя хоста) идентифицирует сервер, на котором размещен ресурс. Это может быть IP-адрес или доменное имя, например, www.example.com.

Порт. Номер порта используется для идентификации конкретного процесса или службы на сервере, которая обрабатывает запрос. Например, HTTP-трафик обычно использует порт 80, а HTTPS-трафик - порт 443.

*Путь***.** Путь определяет конкретное местоположение ресурса на сервере, например /images/logo.png.

Строка запроса. Строка запроса используется для передачи дополнительных параметров или данных на сервер, таких как условия поиска или предпочтения пользователя. Обычно она обозначается знаком вопроса, за которым следуют пары ключ-значение, например? q=digital+forensics.

*Фрагмент***.** Фрагмент (также известный как якорь) используется для идентификации определенного раздела ресурса, например, конкретного заголовка или абзаца на веб-странице. Обычно он обозначается хэш-символом, за которым следует название раздела, например #section1.

IP-адрес.

IP-адрес (числовой идентификатор, который присваивается каждому устройству, подключенному к сети) используется для идентификации и связи с устройствами в Интернете и является важной частью инфраструктуры Интернета.

IP-адреса используются для идентификации отправителя и получателя интернет-трафика, включая электронную почту, запросы веб-страниц и передачу файлов. Каждому устройству, подключенному к Интернету, включая компьютеры, серверы, смартфоны и планшеты, присваивается уникальный IP-адрес.

IP-адреса используются специалистами для определения происхождения и назначения сетевого трафика, а также для отслеживания деятельности отдельных лиц и организаций в Интернете. Анализируя IP-адреса, содержащиеся в сетевом трафике, заголовках электронной почты и других цифровых данных, можно определить географическое положение устройств, выявить модели поведения и проследить поток информации между различными устройствами и сетями.

Однако важно напомнить, что IP-адреса могут быть подделаны или скрыты с помощью прокси-серверов, виртуальных частных сетей (VPN) и других методов. Это означает, что IP-адреса должны использоваться как один из многих инструментов в установлении лиц, совершивших преступления, и должны быть подтверждено другими видами доказательств для создания полной картины деятельности злоумышленника в сети Интернет.

Адрес управления доступом к среде (MAC).

MAC (Media Access Control, уникальный идентификатор, присвоенный сетевому интерфейсу устройства). Каждое устройство, подключаемое к сети, включая компьютеры, смартфоны и другие сетевые устройства, имеет MAC-адрес.

MAC-адреса используются сетевыми администраторами для контроля доступа к сетевым ресурсам и мониторинга сетевого трафика в целях безопасности. Они являются важным компонентом сетевой инфраструктуры и используются широким спектром устройств и приложений для связи друг с другом.

MAC-адреса могут использоваться для отслеживания действий конкретного устройства в компьютерной сети. Анализируя сетевой трафик, можно определить MAC-адрес устройства и отследить его перемещение и действия в компьютерной сети. Это может быть полезно для определения источника сетевых атак, несанкционированного доступа и др.

Важно отметить, что MAC-адреса могут быть подделаны, то есть злоумышленник может изменить MAC-адрес устройства, чтобы создать впечатление, что это другое устройство. Это может затруднить точную идентификацию и отслеживание действий конкретного устройства в сети.

Цифровой сертификат.

Цифровой сертификат *(сертификат SSL/TLS или сертификат X.509) – это цифровой документ, подтверждающий субъекта, например, веб-сайта или физического лица.*

Он выдается доверенным сторонним центром сертификации (ЦС) и содержит такую информацию, как открытый ключ организации, имя организации и ЦС, выдавший сертификат.

Цифровые сертификаты используются в различных контекстах, но их основным назначение является установление безопасного и зашифрованного соединения между клиентом и сервером в Интернете. Когда пользователь заходит на сайт, на котором установлен цифровой сертификат, его браузер проверяет сертификат, чтобы убедиться, что он действителен и выдан доверенным центром сертификации. Если сертификат действителен, браузер устанавливает безопасное соединение с сервером и шифрует все данные, которыми обмениваются клиент и сервер.

Цифровые сертификаты являются важным инструментом в установлении лица, совершившего преступление, поскольку они могут использоваться для проверки принадлежности веб-сайта или физического лица, а также для подтверждения подлинности цифровых подписей.

При раскрытии киберпреступлений цифровые сертификаты могут помочь определить источник вредоносной активности, отследить перемещение данных через Интернет и проверить подлинность компьютерной информации.

В свою очередь цифровые сертификаты могут быть также подделаны, а значит, не следует полагаться на них как на единственный метод проверки подлинности веб-сайта или физического лица. Необходимо использовать различные инструменты и методы, чтобы подтвердить компьютерную информацию и составить полную картину деятельности злоумышленника.

Агент пользователя (User-agent).

Агент пользователя (User-agent) *– это строка информации, которая отправляется веб-браузером или другим программным приложением на веб-сервер при запросе веб-страницы или другого интернет-ресурса.*

User-agent предоставляет информацию о клиентском устройстве и программном обеспечении, используемом для выполнения запроса. Эта информация может быть ценной при проведении осмотра, поскольку она может помочь лицам, производящий осмотр определить источник HTTP-запроса и потенциально связать его с конкретным пользователем или устройством.

Строки агента пользователя обычно содержат такую информацию, как операционная система, веб-браузер и номер версии. Например, строка user-agent для запроса, сделанного с помощью Google Chrome на устройстве с Windows 10, может выглядеть следующим образом:

«Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, как Gecko) Chrome/72.0.3626.81 Safari/537.36».

Возможно использовать строки агента пользователя для реконструкции цифровой деятельности пользователя. Например, если строка агента пользователя указывает, что запрос был сделан с помощью определенного веб-браузера и номера версии, можно определить, использовалась ли известная уязвимость в этом браузере для эксплуатации системы. Кроме того, если строка агента пользователя указывает на то, что запрос был сделан с помощью мобильного устройства, возможно сузить круг поиска до устройств определенного типа или операционной системы.

Однако важно отметить, что строки агента пользователя могут быть изменены пользователями и могут быть ненадежными индикаторами истинного источника запроса. Кроме того, некоторые инструменты и методы, такие как VPN, могут скрывать или манипулировать строками агента пользователя. Тем не менее, во многих случаях строки пользовательских агентов могут предоставить важную информацию и являются важным инструментом в анализе компьютерной информации.

Существует несколько типов агентов пользователя, каждый из которых предоставляет информацию об устройстве и программном обеспечении, используемом для доступа к определенному сайту или ресурсу.

Наиболее распространенные типы агентов пользователя:

Агенты пользователя веб-браузера – тип агентов пользователя, который предоставляет информацию о веб-браузере, используемом для доступа

к веб-сайту или ресурсу. Примерами являются Mozilla Firefox, Google Chrome и Microsoft Edge.

Агенты пользователя мобильных устройств – агенты пользователя используются мобильными устройствами для доступа к веб-сайтам или ресурсам. Они предоставляют информацию об операционной системе, аппаратном обеспечении и браузере мобильного устройства. Примерами являются Apple iOS, Google Android и Windows Mobile.

Агенты пользователя для веб-краулинга или веб-скраппинга – агенты пользователя используются автоматизированными инструментами для сканирования веб-сайтов или сбора данных с них. Примеры: Googlebot, Bingbot и WebCrawler.

Агенты пользователя менеджера загрузки – агенты пользователя используются менеджерами загрузки или ускорителями для загрузки файлов с веб-сайтов. Примеры: IDM (Internet Download Manager), Free Download Manager и Download Accelerator Plus.

Агенты пользователя клиента электронной почты – агенты пользователя используются почтовыми клиентами для отправки и получения сообщений электронной почты. Примеры: Microsoft Outlook, Mozilla Thunderbird и Apple Mail.

Агенты пользователей игровых консолей – агенты пользователя используются игровыми консолями для доступа к игровым онлайн-сервисам и контенту. Примеры: PlayStation Network, Xbox Live и Nintendo Online.

Агенты пользователя виртуального помощника – агенты пользователя используются виртуальными помощниками, такими как Siri, Alexa и Google Assistant, для доступа к веб-сайтам или выполнения задач от имени пользователей.

Каждый тип пользовательских агентов предоставляет различную информацию об устройстве и программном обеспечении, используемом для доступа к определенному ресурсу, и может использоваться для выявления потенциальных уязвимостей безопасности или других проблем при проведении осмотра компьютерной информации.

Агенты пользователя могут выглядеть по-разному на разных устройствах и платформах. Вот несколько примеров того, как агенты пользователя могут выглядеть на разных устройствах:

Настольный или портативный компьютер. Агент пользователя настольного или портативного компьютера обычно содержит информацию об операционной системе и используемом браузере.

Например, строка агента пользователя для устройства с Windows 10, использующего Google Chrome, может выглядеть следующим образом:

«Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, как Gecko) Chrome/72.0.3626.81 Safari/537.36».

Мобильный телефон. Агент пользователя мобильного телефона обычно содержит информацию об операционной системе устройства и используемом мобильном браузере.

Например, строка агента пользователя для iPhone, использующего Safari, может выглядеть следующим образом:

«Mozilla/5.0 (iPhone; CPU iPhone OS 12_1, как Mac OS X) AppleWebKit/605.1.15 (KHTML, как Gecko) Version/12.0 Mobile/15E148 Safari/604.1».

Планшет. Агент пользователя планшета может содержать информацию, аналогичную агенту пользователя мобильного телефона, но может также включать сведения о размере и разрешении экрана.

Например, строка агента пользователя для iPad, использующего Safari, может выглядеть следующим образом:

«Mozilla/5.0 (iPad; CPU OS 12_1, как Mac OS X) AppleWebKit/605.1.15 (KHTML, как Gecko) Version/12.0 Mobile/15E148 Safari/604.1».

Smart TV. Агент пользователя смарт-телевизора может содержать подробную информацию о производителе и модели телевизора, а также об используемой операционной системе и браузере.

Например, строка агента пользователя для телевизора Samsung Smart TV, использующего браузер Tizen, может выглядеть следующим образом:

«Mozilla/5.0 (SMART-TV; X11; Linux armv7l) AppleWebKit/537.42 (KHTML, как Gecko) Chromium/53.0.2785.34 Safari/537.42».

Как видно каждый агент содержит массив информации об устройстве, однако если с устройством, указанным в первых скобках, то происхождение и значение остальной информации требует разъяснения.

«Mozilla/5.0» – часть строки агента пользователя, которая идентифицирует маркер агента пользователя браузера. Эта строка первоначально использовалась Netscape Navigator для идентификации веб-серверов, но с тех пор она стала стандартной строкой агента пользователя для большинства веб-браузеров. Строка «Mozilla/5.0» указывает на то, что браузер совместим с Mozilla, которая является проектом веб-браузера с открытым исходным кодом.

Эта строка включена в современные агенты пользователя по соображениям совместимости, даже если больше нет необходимости указывать на совместимость с Mozilla. Важно отметить, что наличие «Mozilla/5.0» в строке агента пользователя не обязательно означает, что браузер является браузером Mozilla или каким-либо образом связан с организацией Mozilla.

«AppleWebKit/537.42» является частью строки агента пользователя и предоставляет информацию о движке рендеринга, используемом браузером. WebKit – это движок веб-браузера с открытым исходным кодом, используемый многими популярными веб-браузерами, такими как Safari, Chrome и Opera. Число, следующее за версией WebKit, указывает на конкретную сборку движка, используемую браузером.

Например, в строке агента пользователя «Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, как Gecko) Chrome/72.0.3626.81 Safari/537.36», «AppleWebKit/537.36» означает, что браузер использует движок WebKit версии 537.36. Эта информация может быть полезна для при идентификации браузера и возможной привязке его к конкретному устройству или пользователю.

«Chrome/72.0.3626.81» – часть строки агента пользователя, которая идентифицирует конкретный используемый веб-браузер. В данном случае «Chrome» означает веб-браузер Google Chrome, который является одним из самых популярных веб-браузеров, используемых в настоящее время. Число «72.0.3626.81» указывает на конкретную используемую версию Chrome, где

«72.0» – номер основной версии, «3626» - номер сборки, а «81» – номер исправления.

Также может возникнуть вопрос почему в строке агента используются два различных браузера, как например строка «Chrome/72.0.3626.81 Safari/537.36» используется в браузере Google Chrome на базе операционной системы Windows 10. Данная ситуация связана с тем, что Google Chrome – кроссплатформенный веб-браузер, который доступен для различных операционных систем, включая Windows 10. Когда Google Chrome установлен на компьютере с Windows 10, он использует стандартную строку агента пользователя операционной системы, которая включает в себя как «Chrome/72.0.3626.81», так и «Safari/537.36».

Причина включения «Safari/537.36» в строку агента пользователя Google Chrome на Windows 10 заключается в том, что и Google Chrome, и Safari используют один и тот же механизм рендеринга под названием WebKit.

Таким образом, агенты пользователя могут предоставить ценную информацию для криминалистов, помогая им определить источник HTTP-запроса и потенциально связать его с конкретным пользователем или устройством.

Цифровой отпечаток (fingerprint).

Цифровой отпечаток означает уникальный идентификатор, который может быть использован для привязки компьютерной информации к конкретному устройству. Цифровые отпечатки могут быть получены с помощью различных методов, включая хеширование файлов, анализ сети и профилирование устройств.

Одним из распространенных методов создания цифровых отпечатков является **хэширование файлов**. При этом используется математический алгоритм для создания уникального кода, известного как хэш-значение, для файла или фрагмента данных. Затем это хэш-значение можно использовать для сравнения двух файлов или частей данных, чтобы определить, идентичны ли они. Если два файла имеют одинаковое хэш-значение, они считаются идентичными, и это может быть использовано в качестве доказательства для связи файлов с конкретным устройством или человеком.

Еще один метод создания цифровых отпечатков – **анализ сети**. Анализируя сетевой трафик, можно выявить уникальные шаблоны и характеристики, связанные с конкретным устройством или человеком. Эта информация может быть использована для создания сетевого отпечатка, который затем может быть использован для отслеживания действий устройства или человека в сети.

Профилирование устройств – это еще один метод создания цифрового отпечатка. Анализируя аппаратные и программные характеристики устройства, специалисты могут создать уникальный профиль устройства, который затем может быть использован для его идентификации в будущем. Эта информация может быть полезна при выявлении источника атак, киберпреступлений и других видов цифровой деятельности.

Цифровые отпечатки являются важным инструментом в установлении лица, совершившего преступление (идентификации пользователя сети Интернет), поскольку с их помощью можно связать имеющиеся цифровые следы с конкретным устройством, а в последующем и человеком.

Криптокошельки. Криптокошельки – это программные приложения, которые позволяют пользователям безопасно хранить и управлять своей криптовалютой. Они могут использоваться для отправки и получения платежей, отслеживания остатков на счетах и управления несколькими криптовалютными счетами. Кошельки могут быть важным источником информации при выявлении киберпреступлений. Существует несколько типов цифровых кошельков, доступных пользователям для хранения и управления своей криптовалютой.

Программные кошельки – цифровые кошельки, которые загружаются и устанавливаются на компьютер или мобильное устройство пользователя.

Они обычно бесплатны для загрузки и могут использоваться для хранения и управления различными видами криптовалюты. Примерами программных кошельков являются Exodus, Jaxx и Electrum.

Аппаратные кошельки – физические устройства, предназначенные для хранения цифровых активов в автономном режиме.

Они считаются более безопасными, чем программные кошельки, поскольку не подключены к Интернету и поэтому менее подвержены взлому или кибератакам. Примерами аппаратных кошельков являются Trezor, Ledger Nano S и KeepKey.

Веб-кошельки – цифровые кошельки, которые размещаются на стороннем сервере и доступны через веб-браузер.

Они удобны в использовании, поскольку доступ к ним можно получить из любого места, но считаются менее безопасными, чем программные или аппаратные кошельки, поскольку закрытые ключи хранятся на удаленном сервере. Примерами веб-кошельков являются MyEtherWallet, Coinbase и Blockchain.info.

Бумажные кошельки – физические листы бумаги, содержащие открытые и закрытые ключи, необходимые для доступа к криптовалюте и управления ею.

Они считаются очень безопасными, поскольку не подключены к Интернету и поэтому менее подвержены взлому или кибер-атакам. Однако они также менее удобны в использовании, поскольку требуют ручного ввода закрытых ключей. Примерами бумажных кошельков являются BitAddress и WalletGenerator.net.

Мобильные кошельки – цифровые кошельки, специально разработанные для использования на мобильных устройствах.

Они обычно бесплатны для загрузки и могут использоваться для хранения и управления различными видами криптовалюты. Примерами мобильных кошельков являются Bread, Mycelium и Edge.

5.2. Средства компьютерной техники как источники компьютерной информации

В современных условия компьютерное оборудование играет важнейшую роль при выявлении (раскрытии) практически всех преступлений, при совершении которых так или иначе используется компьютерная техника. Поскольку на устройствах хранится большон количество информации, лицам, осуществляющим осмотр компьютерной техники необходимо знать широкий спектр компьютерного оборудования, которое может потребоваться осмотреть.

Настольные компьютеры. Настольные компьютеры являются распространенным источником компьютерной информации.

Можно выделить несколько типов настольных компьютеров, каждый из которых предназначен для различных целей и пользователей. Стоит отметить, что указанные устройства представлены системным блоком, а устройства вывода выступают как вспомогательные элементы и работа компьютера никак не влияет на наличие или отсутствие устройств вывода. Вот некоторые из наиболее распространенных типов настольных компьютеров:

Tower Desktops *(«башня»)* – это наиболее традиционный и распространенный тип доступных настольных компьютеров. Как правило, это самый большой тип настольных компьютеров, предлагающий наибольшую гибкость в плане конфигурации и возможности модернизации;

All-in-One Desktops *(«все в одном»)* – настольные компьютеры «все в одном» разработаны для того, чтобы быть более компактными и занимать меньше места, чем традиционные настольные компьютеры типа «башня». Они объединяют компьютерные компоненты и монитор в единый блок;

Mini Desktops *(«мини»)* – мини-десктопы еще более компактны, чем настольные компьютеры «все в одном», и предназначены для экономии места. Они, как правило, имеют менее мощные компоненты и подходят для выполнения базовых вычислительных задач;

Gaming Desktops *(«игровой»)* – игровые настольные компьютеры разработаны специально для геймеров и оснащены высокопроизводительными

компонентами для обеспечения наилучших игровых возможностей. Они обычно оснащены мощными видеокартами, большим объемом оперативной памяти и быстрыми процессорами;

Workstation Desktops *(«рабочая станция»)* – настольные компьютеры для рабочих станций предназначены для профессионалов, которым необходимо запускать сложные программы и приложения, например, графических дизайнеров, видеоредакторов и др. Они оснащены мощными компонентами и большим объемом оперативной памяти для выполнения сложных рабочих нагрузок;

Business Desktops *(«бизнес»)* – настольные компьютеры для бизнеса предназначены для использования в офисной среде и, как правило, имеют базовые компоненты и функции. Они разработаны для обеспечения надежности и простоты управления в бизнес-среде.

Визуальное представленные устройства выглядят примерно одинаково, отличаясь лишь габаритами.

Ноутбуки похожи на настольные компьютеры, имеют аналогичную структуру и типизацию, а также содержат внутренние компоненты, которые могут представлять интерес в качестве источников компьютерной информации. Жесткий диск и другие устройства хранения данных, встроенные в ноутбуки, могут содержать информацию, которая имеющую значение.

Серверы используются для хранения и управления большими объемами данных и могут содержать важную компьютерную информацию. Лицам, производящим осмотр может понадобиться проанализировать данные на сервере, включая файлы журналов и действия пользователей и др.

По видам серверов представляется возможным привести следующую классификацию:

резервные серверы – серверы, содержащие резервные копии данных как с различных информационных систем, так и других серверов;

административные серверы – серверы, на которых содержится информация о работе информационных систем организаций;

веб-серверы **–** серверы, на которых размещаются веб-сайты и может содержаться соответствующая информация, относящаяся к преступлению,

например, веб-журналы и базы данных. Серверы могут быть подвергнуты осмотру для получения информации о действиях пользователей или для выявления потенциальных нарушений безопасности;

серверы электронной почты – серверы, которые управляют электронной почтой и могут содержать соответствующую информацию, относящуюся к преступлению, например, сообщения электронной почты и вложения. Хранящаяся компьютерная информация может быть проанализирована для установления схем коммуникации при осуществлении незаконной деятельности.

Центральные процессоры с позиции обнаружения значимой компьютерной информации обычно не делятся на различные виды, однако существуют различные типы архитектур центрального процессора, которые могут иметь значение для осмотра указанных устройств. Вот несколько примеров:

архитектура x86 – широко распространенная архитектура центрального процессора, которая используется в большинстве настольных и портативных компьютеров. Лицам, производящим осмотр важно знать эту архитектуру, поскольку многие инструменты осмотра предназначены для работы с системами на базе x86;

архитектура ARM – архитектура процессора, которая обычно используется в мобильных устройствах, таких как смартфоны и планшеты, также используется в некоторых встраиваемых системах;

энергетическая (power) архитектура – архитектура процессора, которая используется в некоторых серверных системах, а также в некоторых встраиваемых системах.

Также существует множество других используемых архитектур процессоров, таких как MIPS и SPARC, которые реже представлены в различных информационных системах и редко являются объектами осмотра.

Материнская плата имеет определенные характеристики и компоненты, которые необходимо учитывать при обнаружении и анализе компьютерной информации при установлении лица, совершившего преступление. Так, например:

чипсет – ключевой компонент материнской платы, который управляет обменом данными между процессором, памятью и периферийными устройствами. Чипсет может влиять на производительность и функциональность компьютерной системы, а также на способ хранения и доступа к данным. Лицам, производящим осмотр может потребоваться изучить набор микросхем, чтобы правильно проанализировать и интерпретировать данные, хранящиеся в системе;

BIOS *(Basic Input/Output System) или UEFI (Unified Extensible Firmware Interface)* – микропрограмма, управляющая процессом загрузки компьютерной системы.

Она хранится в микросхеме на материнской плате и отвечает за инициализацию оборудования и загрузку операционной системы. BIOS/UEFI может содержать значимую компьютерную информацию, например, параметры конфигурации системы, информацию об оборудовании и пароли пользователей;

слоты расширения: материнские платы могут иметь слоты расширения для установки дополнительных компонентов, таких как видеокарты, сетевые карты или устройства хранения данных. Лицам, производящим осмотр необходимо знание типов слотов расширения, доступных на материнской плате, чтобы правильно анализировать и интерпретировать данные, хранящиеся на этих устройствах;

встроенная память: некоторые материнские платы могут иметь встроенные устройства хранения данных, такие как флэш-память или жесткие диски. Эти устройства могут хранить значимую для анализа информацию, такую как, например, системные журналы, пользовательские данные.

Накопители информации можно разделить на различные виды в зависимости от их технологии и форм-фактора.

Жесткие диски (HDD – Hard Disk Drives) являются наиболее распространенным типом накопителей данных и используют магнитные диски для хранения данных, они различаются по форм-фактору[15], емкости, скорости вращения и интерфейсу;

[15] Форм-фактор – стандарт технического изделия, описывающий некоторую совокупность его технических параметров.

Существуют определенные особенности и характеристики жестких дисков, которые могут иметь значение для обнаружения и анализа компьютерной информации. Вот несколько примеров:

форм-фактор: жесткие диски бывают разных физических форм-факторов, например, 2,5- или 3,5-дюймовые, что необходимо учитывать для правильного анализа хранящейся информации;

интерфейс: используются различные интерфейсы для подключения к компьютерной системе, например, SATA, SCSI или SAS, что необходимо учитывать для правильного подключения диска к рабочей станции и последующего осмотра;

емкость: жесткие диски бывают разной емкости от нескольких гигабайт до нескольких терабайт, что влияет на объем хранящейся информации и на время, необходимое для ее анализа;

данные S.M.A.R.T (Self-Monitoring, Analysis and Reporting Technology) – это система, которая следит за состоянием и производительностью жесткого диска и содержит информацию, которую необходимо учитывать, например, количество циклов питания или объем данных, записанных на диск.

В ***твердотельных накопителях (SSD – Solid State Drives)*** для хранения данных используется флэш-память, и они не имеют движущихся частей. Твердотельные накопители обычно быстрее жестких дисков и все чаще используются в современных компьютерных системах, могут быть более сложными для анализа из-за таких функций, как выравнивание износа и команды обрезки;

Твердотельные накопители (SSD) можно разделить на различные виды в зависимости от их технологии и особенностей, которые могут повлиять на процесс обнаружения и анализа компьютерной информации:

твердотельные накопители SATA (Serial Advanced Technology Attachment) являются наиболее распространенным типом твердотельных накопителей и подключаются к компьютерной системе с помощью интерфейса SATA. В них могут использоваться различные типы флэш-памяти NAND, включая одноуровневые ячейки (SLC), многоуровневые ячейки (MLC) и трехуровневые ячейки (TLC), что влияет на их скорость и долговечность.

Твердотельные накопители SATA также могут поддерживать такие функции, как шифрование;

твердотельные накопители NVMe: твердотельные накопители NVMe (Non-Volatile Memory Express) – более новый тип твердотельных накопителей, которые используют интерфейс NVMe для подключения к компьютерной системе. Твердотельные накопители NVMe могут обеспечивать более высокую скорость чтения и записи, чем твердотельные накопители SATA, и могут дополнительные функции безопасности;

твердотельные накопители M.2: тип твердотельных накопителей, использующих форм-фактор M.2 для подключения к компьютерной системе. Твердотельные накопители M.2 могут использовать интерфейс SATA или NVMe и могут иметь различную емкость и средства защиты;

твердотельные накопители PCIe (Peripheral Component Interconnect Express) используют интерфейс PCIe для подключения к компьютерной системе и могут обеспечивать еще более высокую скорость чтения и записи, чем твердотельные накопители NVMe, могут иметь различные уровни шифрования и другие функции безопасности;

самошифрующиеся твердотельные накопители имеют встроенные функции шифрования, которые могут защитить данные на диске от несанкционированного доступа, использовать аппаратное шифрование или программное обеспечение для шифрования, и для доступа к данным в ходе осмотра (исследования) могут потребоваться специальные инструменты или программное обеспечение.

Оптические диски такие как CD, DVD и Blu-ray, могут хранить данные в цифровом формате, используя лазер для чтения и записи данных. Оптические диски могут быть полезны для хранения больших объемов данных, но они становятся все менее распространенными по мере появления новых технологий хранения данных.

USB-накопители – это небольшие и портативные устройства хранения данных, в которых для этих целей используется флэш-память. USB-накопители обычно используются для переноса данных между системами или для резервного копирования.

Карты памяти – это небольшие портативные устройства хранения данных, использующиеся в цифровых камерах, смартфонах и других электронных устройствах. В картах памяти могут использоваться различные технологии, например, флэш-память или карты SD.

Необходимо отметить, что специфические характеристики каждого накопителя данных могут повлиять на процесс обнаружения компьютерной информации, например, время, необходимое для анализа накопителя, и методы, используемые для восстановления данных с него.

Мобильные устройства, такие как смартфоны и планшеты, все чаще используются для хранения и доступа к различным данным. Эти устройства могут содержать значимую информацию, например, текстовые сообщения, журналы вызовов и историю просмотра интернет-страниц.

Мобильные устройства можно разделить на различные типы в зависимости от их операционной системы, архитектуры и средств защиты.

Устройства Android. Android – это операционная система с открытым исходным кодом, разработанная компанией Google и используемая различными мобильными устройствами. Устройства Android могут иметь различную аппаратную архитектуру, например, ARM или x86, различные функции безопасности, такие как шифрование и безопасная загрузка, которые могут повлиять на процесс осмотра;

Устройства iOS. iOS – это операционная система с закрытым исходным кодом, разработанная компанией Apple и используемая исключительно в мобильных устройствах Apple. Устройства iOS имеют специфическую аппаратную архитектуру и функции безопасности, такие как secure enclave и Touch ID/Face ID. Устройства iOS также имеют функцию под названием «Secure Bootchain», которая значительно затрудняет модификацию прошивки устройства;

устройства Windows Mobile. Windows Mobile – это операционная система с закрытым исходным кодом, разработанная компанией Microsoft и используемая различными мобильными устройствами. Мобильные устройства Windows могут иметь различную аппаратную архитектуру, например, ARM или

x86 и различные функции безопасности, такие как шифрование и безопасная загрузка;

устройства Blackberry. Blackberry – это операционная система с закрытым исходным кодом, разработанная компанией BlackBerry Limited и используемая различными мобильными устройствами. Устройства Blackberry имеют специфическую аппаратную архитектуру и функции безопасности, такие как Blackberry Balance и зашифрованное хранение данных;

гибридные устройств. Некоторые мобильные устройства, такие как Microsoft Surface, можно считать гибридными устройствами, поскольку они могут функционировать как планшет и ноутбук. Эти устройства могут иметь различную аппаратную архитектуру, операционные системы и средства защиты.

Сетевое оборудование. Сетевое оборудование, такое как маршрутизаторы и коммутаторы, также может потребоваться осмотреть в ходе проведения проверок по материалам и при установлении лица, совершившего преступление. Эти устройства могут содержать данные, например, о сетевом трафике и действиях пользователей.

Сетевое оборудование можно разделить на различные виды в зависимости от их функций и использования:

маршрутизаторы – это сетевые устройства, которые направляют трафик между различными сетями. Они используют такие протоколы, как IP и ARP, для определения наилучшего пути передачи данных между различными устройствами;

коммутаторы – это сетевые устройства, которые соединяют несколько устройств в сети, используют MAC-адреса для направления трафика на определенные устройства в сети;

брандмауэры – это сетевые устройства, которые контролируют доступ к сети путем фильтрации входящего и исходящего трафика на основе заранее определенных правил;

системы обнаружения и предотвращения вторжений (IDS/IPS) – это сетевые устройства, которые отслеживают сетевой трафик на предмет признаков вредоносной активности и могут предупреждать сетевых

администраторов или предпринимать действия по блокированию такой активности;

прокси-серверы – это сетевые устройства, которые выступают в качестве посредников между клиентами и серверами. Используются для фильтрации трафика, кэширования данных или обеспечения анонимности для клиентов.

Принтеры и сканеры могут содержать данные, связанные с заданиями на печать, такие как дата и время задания на печать и пользователь, который его инициировал. Эта информация может быть использована для определения того, кто имел доступ к документам.

Принтеры и сканеры можно разделить на различные типы в зависимости от их технологии и использования:

струйные принтеры создают изображения путем распыления крошечных капель чернил на бумагу;

лазерные принтеры используют тонер для создания изображений путем переноса электростатически заряженного порошка на бумагу;

матричные принтеры создают изображения, ударяя красящей лентой по бумаге, в результате чего образуется серия точек;

планшетные сканеры используются для сканирования документов и изображений, преобразуя их в цифровые файлы;

листовые сканеры используются для сканирования документов и изображений, подавая их через сканер по одной странице за раз;

3D-принтеры создают физические объекты путем наложения слоев материала, например, пластика или металла, на основе цифровой модели.

Системы резервного копирования, такие как облачные хранилища и ленточные системы резервного копирования, также могут содержать компьютерную информацию, имеющих значение для установления лица, совершившего преступлений.

Системы резервного копирования можно разделить на несколько видов:

ленточные системы резервного копирования используют магнитную ленту для хранения копий данных с компьютеров или серверов;

дисковые системы резервного копирования используют жесткие диски или другие магнитные носители для хранения копий данных с компьютеров или серверов;

облачные системы резервного копирования хранят копии данных на удаленных серверах, как правило, через стороннего поставщика;

зеркальные системы резервного копирования создают точные копии данных в режиме реального времени, как правило, используя два или более жестких диска;

инкрементные системы резервного копирования хранят копии данных, которые изменились с момента создания последней резервной копии;

системы моментального резервного копирования: системы резервного копирования моментальных снимков создают точечную копию данных, позволяя пользователям восстанавливать данные до определенного момента времени.

Электронные коммуникационные устройства (серверы электронной почты и службы мгновенного обмена сообщениями) также могут представлять интерес как источник компьютерной информации, могут содержать информацию, связанную с общением между людьми, в том числе при совершении преступлений.

Виды серверов электронной почты и службы мгновенного обмена сообщениями:

серверы электронной почты используются для отправки и получения сообщений электронной почты;

службы мгновенного обмена сообщениями (мессенджеры) используются для отправки текстовых сообщений в режиме реального времени через Интернет;

услуги голосовых и видеочатов используются для аудио- и видеосвязи в режиме реального времени через Интернет;

платформы социальных сетей используются для общения, обмена контентом и создания онлайн-сетей;

файлообменные сервисы используются для обмена файлами через Интернет;

виртуальные частные сети (VPN) используются для создания безопасного и зашифрованного соединения между двумя или более устройствами через Интернет.

5.3. Особенности осмотра средств компьютерной техники и компьютерной информации: программно-технические аспекты

Осмотр начинается с определения целей, которые задают направление поиска, определяют выбор методов и необходимых инструментов. Правильная постановка цели способствует быстрому и эффективному достижению желаемого результата. В контексте осмотра СКТ и компьютерной информации, можно разбить главную цель на более мелкие и простые компоненты. Таким образом, разделение цели на конкретные задачи позволяет определить необходимые действия и приводит к постепенному сбору ее фрагментов, необходимых для ее решения.

Осмотр компьютерной информации (мобильного устройства, другого СКТ) проводится в присутствии владельца устройства с его согласия либо по постановлению о производстве осмотра, санкционированного прокурором (ст. 204-1 УПК Республики Беларусь) либо при осуществлении оперативно-розыскной деятельности. Наличие таких сведений в тексте электронного сообщения, позволяет немедленно приступить к проведению оперативно-розыскных мероприятий. Одним из самых эффективных и доступных является оперативно-розыскное мероприятие «оперативный осмотр». Согласно ст. 26 Закона «Об оперативно-розыскной деятельности», оперативный осмотр представляет собой обследование жилища и иного законного владения гражданина, помещения, здания, сооружения, транспортного средства, иного объекта и территории организации, участка местности, а также изучение информационных систем, информационных ресурсов, предметов и документов, компьютерной информации, в том числе путем удаленного доступа, в целях получения сведений, необходимых для выполнения задач оперативно-розыскной деятельности. В ходе проведения может осуществляться копирование, изъятие предметов и документов, компьютерной информации (например, изъятие архива истории telegram-чата и др.).

В целях достижения целей осмотра СКТ и компьютерной информации необходимо определить тактические ситуации, возникающие при подобного

рода мероприятиях, которые обусловливают использование различных способов обнаружения и анализа.

Информацию, полученную в ходе проведенного осмотра, необходимо помещать в таблицу фотоснимков, а также на МНИ, которые приобщать к протоколу осмотра.

Начнем с более общих тактических ситуаций, когда объект исследования находится:

непосредственно на месте происшествия;

в служебном помещении лица, производящего осмотр;

в глобальной компьютерной сети.

В случаях, когда исследуемое устройство находится непосредственно на месте происшествия и в служебном помещении представляется возможным выделить еще две тактические ситуации:

устройство находится во включенном состоянии;

устройство находится в выключенном состоянии.

Также различие способов исследования имеет место, когда устройство принадлежит либо потерпевшему, либо подозреваемому.

Рассмотрим ситуацию, когда исследуется устройство потерпевшего. В этом случае основной целью является установление хронологии конкретного события в цифровом пространстве. Для достижения этой цели необходимы ответы на следующие вопросы:

как злоумышленник получил доступ к системе;

какие инструменты были использованы;

смог ли злоумышленник закрепиться в системе;

произошло ли сетевое распространение;

какие действия были выполнены в целевой системе.

В свою очередь, при установлении хронологии доступа злоумышленника к системе можно выделить ряд других вопросов, требующих разрешения:

имеются ли следы открытия потенциально вредоносных файлов или ссылок;

использовались ли сервисы для удаленного подключения;

есть ли подозрительные сетевые подключения;

есть ли следы подключения съемных устройств.

Аналогично, в вопросе о вредоносных файлах:

есть ли следы сохранения подозрительных файлов?

есть ли следы открытия подозрительных ссылок?

есть ли следы открытия подозрительных файлов?

Ответы на эти вопросы требуют не только знания цифровых следов и их источников, но и тактики, техники и методов, используемых злоумышленниками. Разбивая каждый вопрос верхнего уровня до этого уровня, можно получить список простых вопросов с однозначными ответами, что позволяет составить полную картину события.

Аналогичный метод можно использовать для исследования устройства, с которого предположительно была инициирована атака. В этом случае вопросы должны быть основаны на том, в чем подозревается владелец устройства. Например, если он разработал вредоносное программное обеспечение, вопросы должны касаться наличия инструментов разработки, следов исходного кода, продажи вредоносного программного обеспечения и так далее.

Алгоритм проведения осмотра избирается исходя из конкретной тактической ситуации и осматриваемого устройства. Однако при проведении осмотра большинства из СКТ можно придерживаться следующего алгоритма.

Осмотр компьютерной информации, принадлежащей потерпевшему (свидетелю), ограничен видом совершенного преступления и, как правило, не требует исследования во всем объеме.

Основной задачей осмотра в данном случае является решение следующих вопросов:

какая компьютерная информация и каким образом подвергалась преступному воздействию;

какие были пути и способы доступа к ней у подозреваемого (обвиняемого) (например, использование прав администратора (владельца информации), удаленный доступ с использованием компьютерной сети и вредоносных программ и др.);

какие следы несанкционированного доступа к компьютерной информации остались (лог-файлы доступа к информации и ее носителю);

посредством каких компьютерных программ осуществлялась электронная переписка между участниками уголовного процесса (например, подозреваемым - потерпевшим, потерпевшим - свидетелем и т. д.);

кто может располагать сведениями о совершенном преступлении и в каком объеме и др.

Осмотр компьютерной информации, принадлежащей подозреваемому (обвиняемому), является самым объемным и трудоемким, поскольку здесь представляет интерес не только информация о совершенном преступлении, но и иные сведения, которые могут содержать следы других (еще не выявленных) преступлений, а также данные, характеризующие личность подозреваемого (обвиняемого) (например, интерес к компьютерным технологиям, в том числе их возможностям для совершения преступлений, и др.).

К типичным местам хранения значимой информации на жестких магнитных дисках (винчестере) компьютера подозреваемого (обвиняемого) в среде Windows следует отнести:

1) C:\Program Files\ - директория установки по умолчанию всего программного обеспечения, путем осмотра которой можно опре. делить установленные и используемые на компьютере преступника программы;

2) C:\Users*имя пользователя*\AppData\ - директория хранения каталогов установленных на компьютере программ, результаты работы которых в виде файлов можно обнаружить в ходе осмотра (например, электронную переписку посредством почтовых клиентов Microsoft Outlook, The Bat и m. n., посредством сервисов мгновенного обмена сообщениями в интернете ICQ, QIP u m. д.);

3) C:\Users*имя пользователя*\Recent\ - директория хранения в алфавитном порядке временных копий файлов, которые открывались на осматриваемом компьютере последними за определенный период времени (около месяца);

4) C:\Users*имя пользователя*\Documents\ - директория хранения по умолчанию личных документов, а также результатов работы некоторых программ;

5) C:\Users*имя пользователя*\Desktop\ - директория хранения ярлыков программ, файлов, размещенных на рабочем столе осматриваемого компьютера;

6) C:\Users*имя пользователя*\Downloads\ - директория хранения загруженных из интернета файлов;

7) C:\RECYCLER\ - директория хранения удаленных и перемещенных в корзину файлов, из которой они в последующем не удалены;

8) C:\Documents and Settings User*имя пользователя*\AppData\

WebMoney* kwm) или иное место хранения файла «* kwm» (где * - номер идентификатора электронной платежной системы WebMoney) - файл, содержащий идентификационный ключ (WMID) электронной пла-тежной системы WebMoney. Имя файла и будет являться номером используемого преступником WMID (если на компьютере подозреваемого установлена и применялась данная программа);

9) C:\Documents and Settings \User*имя пользователя*\AppData\

WebMoneyl*.pwm\ или иное место хранения файла «* рит» (где * - номер идентификатора электронной платежной системы WebMoney) - файл, содержащий историю входящих/исходящих платежей по кошелькам идентификатора WebMoney;

10) C:\Documents and Settings\User*имя пользователя*\AppData\

Microsoft\Outlook*.PST\ - файл, содержащий результаты работы почтового клиента Microsoft Outlook: электронные письма, адресная книга, органайзер (если на компьютере подозреваемого установлена и использовалась данная программа) и т. д.

В приведенных примерах диск С - системный, который служит для хранения установленной операционной системы и программного обеспечения и определяется в зависимости от предустановленных пользователем компьютера настроек.

В ходе осмотра компьютерной информации, принадлежащей подозреваемому (обвиняемому), могут быть обнаружены:

сведения о подготовке и совершении преступления, а также сокрытии его следов;

информация, которой неправомерно завладел подозреваемый (обвиняемый), либо результаты ее использования;

зафиксированные и сохраненные сведения о жертвах преступлений (например, список номеров банковских платежных карт, с которых совершались хищения денежных средств; список IP-адресов компьютеров, к которым осуществлялся несанкционированный доступ либо которые были заражены распространенными вредоносными программами; списки взломанных идентификаторов кошельков электронных платежных систем и др.);

средства разработки вредоносных программ, использовавшихся при совершении преступления, следы их использования;

данные о создании или регистрации подозреваемым (обвиняемым) в интернете различных аккаунтов (например, личных сайтов, электронных кошельков, электронных почтовых ящиков и т п.):

информация в виде электронных книг, журналов, публикаций, фото-и видеоматериалов, программ и т. д., подтверждающая интерес подозреваемого (обвиняемого) к компьютерным устройствам, программному обеспечению, интернету и их возможностям (в том числе для достижения противоправных целей);

переписка подозреваемого (обвиняемого) в мессенджерах, социальных сетях, по электронной почте и др.

Следует отдельно выделить электронную переписку подозреваемого (обвиняемого), которая является важнейшим источником доказательств. Сложность ее изучения обусловлена прежде всего спецификой и разнообразием компьютерного сленга, включающего элементы криминальных, технических и компьютерных терминов, при помощи которых общаются лица, совершающие преступления против компьютерной безопасности. Как правило, без специальных знаний довольно сложно понять суть переписки соучастников, детали планируемых или совершенных преступлений. Так называемый перевод применяемого сленга целесообразно осуществлять при помощи интернета, даркнета, кардерских сайтов, форумов, а также исходя из информации, полученной при проведении допроса подозреваемого (обвиняемого). При этом

к протоколу осмотра электронной переписки целесообразно прилагать своеобразный словарь используемых в переписке терминов с расшифровкой для их понимания судьей и иными участниками уголовного процесса в ходе судебного разбирательства.

При проведении осмотра средств компьютерной техники на месте происшествия может возникнуть две тактических ситуации:

когда осматриваемое устройство находится во включенном;

или выключенном состояниях.

Осмотр устройства в указанных ситуациях может производится согласно следующему алгоритму:

обеспечение защиты системы и отключение ее от любого сетевого подключения, чтобы предотвратить любой удаленный доступ или модификацию;

документирование информации о системе, включая ее марку, модель и серийный номер;

фото(видео-)фиксация физического состояния системы, включая все кабели, порты и периферийные устройства, подключенные к системе;

документирование конфигурации системы, изучение и фиксация версии операционной системы, прикладного программное обеспечение и любых других соответствующих настроек системы;

включение питания системы и фиксация последовательности загрузки, отмечая любые сообщения об ошибках;

создание образа диска системного носителя, например, жесткого диска или твердотельного накопителя. Образ должен быть побитовой копией оригинального носителя и включать все разделы, нераспределенное пространство и скрытые файлы;

обеспечение хранения образа диска в безопасном месте и проверка его целостности, сравнив хэш-значение с оригинальным носителем;

анализ образа диска с помощью программного обеспечения, для восстановления хронологии событий, а также удаленных, скрытых или зашифрованных файлов, а также выявление признаков вредоносной деятельности.

Исходя из изложенного также необходимо учитывать ряд особенностей, чтобы обнаруженная значимая компьютерная информация была допустима и могла быть использована для установления лица, совершившего преступление.

Сохранение компьютерной информации. Для того, чтобы компьютерная информация не была утеряны или повреждены в процессе осмотра, важно предпринять соответствующие меры по обеспечению ее сохраненности. Это может включать создание битовой копии жесткого диска или другого носителя информации, или фотографирование оборудования до того, как оно будет изъято с места происшествия.

Специализированные инструменты и методы. Для проведения осмотра компьютерного техники часто требуются специальные инструменты и методы, которыми лицо, производящее осмотр, не владеет. Например, для изучения содержимого жесткого диска или восстановления удаленных файлов может потребоваться специализированное программное обеспечение.

Шифрование данных. Шифрование может представлять собой проблему при осмотре компьютерной техники. Доступ к зашифрованным данным может быть затруднен или невозможен без соответствующего пароля или ключа для расшифровки, а попытка подобрать шифр может повредить или удалить данные.

Удаленный доступ. В некоторых случаях можно провести осмотр дистанционно, не прибегая к физическому доступу на место происшествия. Это может быть применимо, когда речь идет об оборудовании, находящемся в другой юрисдикции или в труднодоступном месте.

На первоначальном этапе осмотра необходимо предпринять действия для обеспечения сохранности данных, находящихся на осматриваемых устройствах.

Создание образа либо дампа памяти. Данное действие подразумевает создание побитовой копии носителя информации либо дампа памяти оперативной памяти, которые сохраняют данные и гарантирует, что они не были изменены каким-либо образом. Эта копия может быть использована для проведения осмотра вне пределов места происшествия, что позволяет сохранить оригинальные доказательства.

Использование блокираторов записи. При создании образа необходимо использовать блокираторы записи, чтобы предотвратить внесение изменений в исходные данные. Блокираторы записи гарантируют, что данные не будут изменены или перезаписаны в процессе создания образа.

Создание резервной копии. После создания образа возможно создание его резервной копии и ее хранение. Она может быть использована в случае потери или повреждения оригинального образа.

Создание образа носителя информации либо дампа оперативной памяти

Как упоминалось ранее, данное действие подразумевает создание побитовой копии носителя информации либо дампа памяти оперативной памяти, которые сохраняют данные и гарантирует, что они не были изменены каким-либо образом.

Побитовая копия носителя информации *– это процесс создания точной копии всего содержимого носителя, включая все данные, файловые структуры и метаданные, на самом низком возможном уровне устройства хранения. Этот процесс также известен как «образ диска», «клонирование диска» или «копирование диска».*

При побитовом копировании каждый бит данных на носителе копируется на целевой носитель, независимо от того, являются ли эти данные частью файла, удалены или скрыты, или частью самой файловой системы. В результате создается полная, точная копия исходного носителя, включая все ошибки, несоответствия или повреждения, которые могут присутствовать.

Побитовые копии часто используются для восстановления данных, криминалистических исследованиях или резервном копирования системы. Они позволяют создать полную копию носителя информации, которую затем можно использовать для восстановления потерянных или поврежденных данных, анализа файловых структур или метаданных, а также для сохранения конфигурации системы в целях резервного копирования и аварийного восстановления.

Дамп памяти или дамп ОЗУ *– это процесс копирования содержимого памяти с произвольным доступом (RAM) компьютера на устройство хранения данных, такое как, например, жесткий диск или флэш-накопитель.*

Таким образом создается снимок памяти системы в определенный момент времени. Дампы памяти часто создаются автоматически операционной системой или приложениями в случае сбоя или ошибок системы, они также могут создаваться вручную.

Информация, содержащаяся в дампе памяти, может включать данные запущенных программ, самой операционной системы и любых фоновых процессов или служб. Эти данные можно использовать для выявления причин системных ошибок, диагностики проблем производительности или восстановления потерянных данных.

Однако интерпретация содержимого дампа памяти может быть сложной задачей, поскольку он может содержать большое количество необработанных данных, которые трудно расшифровать без специальных инструментов и знаний.

Для создания побитовой копии носителя информации можно использовать специализированное программное обеспечение, предназначенное для создания образов дисков или клонирования дисков.

Алгоритм создания побитовой копии:

подключить исходный носитель к компьютеру и убедится, что он распознан операционной системой;

подключить целевой носитель к компьютеру и убедится, что на нем достаточно места для размещения всего содержимого исходного носителя;

установить и открыть программу для создания образа диска или клонирования диска;

выбрать опцию создания нового образа диска или клона диска и выбрать исходный носитель в качестве входного;

выбрать целевой носитель в качестве выходного и выбрать опцию создания побитовой копии или точного клона исходного носителя;

запустить процесс копирования и дождаться его завершения. Это может занять некоторое время, в зависимости от размера носителя и скорости компьютера и устройств хранения данных;

после завершения процесса копирования необходимо проверить, что целевой носитель содержит точную копию исходного носителя, сравнив размеры файлов, проверив наличие ошибок или повреждений и убедившись, что данные и их метаданные не повреждены.

Существует множество вариантов **программного обеспечения для создания побитовых копий носителей информации**. Несколько популярных вариантов:

dd – это утилита командной строки, доступная во многих операционных системах на базе Unix[16], которую можно использовать для создания побитовой копии носителя информации. Это инструмент требует определенных знаний синтаксиса командной строки и может быть сложен в использовании;

Clonezilla – это бесплатная программа для создания образов дисков с открытым исходным кодом, которую можно использовать для создания образов дисков или клонов носителей информации. Она поддерживает широкий спектр файловых систем и устройств хранения данных и имеет графический интерфейс;

Macrium Reflect – это коммерческое программное обеспечение для создания образов дисков для Windows, которое предлагает ряд функций для клонирования и резервного копирования дисков, поддерживает широкий спектр устройств хранения данных;

Acronis True Image – это коммерческая программа (имеет бесплатные вариации) для создания образов дисков для Windows, которая предлагает функции клонирования дисков, резервного копирования и аварийного восстановления. Наиболее часто применяется в практической деятельности органов внутренних дел.

[16]Unix - семейство переносимых, многозадачных и многопользовательских операционных систем, которые основаны на идеях оригинального проекта AT&T Unix (например, Linux, Mac OS)

Norton Ghost – это коммерческое программное обеспечение для создания образов дисков для Windows, которое можно использовать для создания образов дисков или клонов носителей информации.

Существует программное обеспечение для создания дампа оперативной памяти (дамп ОЗУ).

FTK Imager – коммерческий инструмент для создания криминалистических изображений от AccessData, который можно использовать для создания дампов памяти, а также образов дисков, имеет широкий набор функций для криминалистического анализа;

WinPmem – бесплатный инструмент сбора данных о памяти с открытым исходным кодом от Volatility Foundation, который можно использовать для создания дампов памяти в системах Windows. Включает интерфейс командной строки и поддерживает широкий спектр операционных систем и архитектур памяти;

Belkasoft Live RAM Capturer – коммерческий инструмент осмотра компьютерной техники, который можно использовать для создания дампов оперативной памяти, а также для анализа и обработки образов памяти.

Рассмотрим **алгоритм создания дампа оперативной памяти** на примере популярных операционных систем.

Использование блокираторов записи. Блокираторы записи, также известные как блокираторы данных или блокираторы данных USB, устройства, которые предотвращают передачу данных между устройством USB и компьютером.

Когда USB-устройство подключается к компьютеру, устанавливается соединение для передачи данных, которое потенциально может передавать данные между устройством и компьютером. Эта передача данных может быть использована для хищения компьютерной информации или установки вредоносного ПО на устройство, что представляет угрозу безопасности. Блокираторы записи работают путем физического блокирования контактов передачи данных в порту USB, предотвращая любую передачу данных и позволяя только передачу энергии для зарядки устройства.

Создание резервной копии. Создание резервной копии системы или хранилища начинается с *определения того, каких данных необходимо создать резервную копию*. Это может быть операционная система, приложения, личные файлы и другие данные.

Выбор метода резервного копирования. Существует несколько методов резервного копирования, например, полное резервное копирование, инкрементное или дифференциальное резервное копирование.

Выбор местоположения резервного копирования. Необходимо выбрать место резервного копирования, которое будет находиться отдельно от основной системы или хранилища, например, внешний жесткий диск.

Выбор программного обеспечение для резервного копирования. Существует множество вариантов программного обеспечения для резервного копирования (например, Acronis True Image, EaseUS Todo Backup и Macrium Reflect).

Настройка параметров резервного копирования таких как тип резервного копирования, частота и место назначения.

Выполнение резервного копирования. В зависимости от выбранного программного обеспечения для резервного копирования это может включать создание резервного образа, копирование файлов или синхронизацию данных между несколькими устройствами.

Существуют различные варианты программного обеспечения для создания резервных копий системы или хранилища. Некоторые популярные варианты включают:

Acronis True Image – комплексное программное обеспечение для резервного копирования и восстановления, которое может создавать полные резервные копии системы, образы дисков и резервные копии файлов. Оно предлагает такие функции, как инкрементное резервное копирование, облачное резервное копирование и клонирование дисков;

EaseUS Todo Backup – программное обеспечение может создавать резервные копии системы, резервные копии дисков/разделов и резервные копии файлов. Оно также предлагает такие функции, как клонирование диска, синхронизация файлов и автоматическое резервное копирование.

Macrium Reflect – программное обеспечение позволяет создавать полные резервные копии системы, образы дисков и резервные копии файлов. Оно предлагает такие функции, как дифференциальное резервное копирование, облачное резервное копирование и клонирование дисков.

Резервное копирование и восстановление Windows – встроенный в Windows инструмент резервного копирования и восстановления может создавать полные резервные копии системы, образы дисков и резервные копии файлов. Он предлагает такие функции, как инкрементное резервное копирование, точки восстановления системы и создание образов дисков.

5.4. Виды и назначение программного обеспечения, используемого при выявлении и раскрытии преступлений

Изложенный в предыдущем разделе перечень программного обеспечения хоть и помогает в решении задач стоящих перед осмотром средств компьютерной техники, тем не менее был разработан для решения задач стоящих перед рядовыми пользователями. Разработка нового программного обеспечения необходима для того, чтобы не отставать от этих изменений и эффективно противодействовать новым формам киберпреступлений.

Для быстрого и в то же время эффективного решения задач по выявлению и раскрытию преступлений должно применяться соответствующее программное обеспечение, позволяющее проводить поиск, выявление и анализ информации.

Рассмотрим характеристику специального программно-технического обеспечения, разработанного для правоохранительных органов и предназначенных для проведения исследований компьютерной техники и компьютерной информации.

«Мобильный криминалист» является инструментом для проведения исследования СКТ и компьютерной информации. Позволяет извлекать информацию из смартфонов, планшетных компьютеров и других персональных устройств, дронов, облачных сервисов. Отдельные программные решения позволяют обнаруживать, извлекать и анализировать информацию из персональных компьютеров. Возможности программы позволяют сотрудникам правоохранительных органов в кратчайшие сроки найти важную компьютерную информацию, имеющую цифровые следы преступления и анализировать ее с помощью разнообразных интегрированных утилит.

Продукты «Мобильный Криминалист» позволяют извлекать и анализировать информацию из следующих устройств:

мобильные устройства: извлечение информации из десятков тысяч различных мобильных устройств, SIM и SD-карт. Позволяет создавать физические и логические образы устройств, извлекать и расшифровывать все

данные, в том числе удаленные, импортировать физические образы и резервные копии устройств, получать данные из дронов и выстраивать маршруты полетов;

облачные хранилища: извлечение информации из большинства популярных облачных сервисов. Позволяет получить доступ к облачным сервисам, используя учетные данные, найденные при изучении информации на мобильных устройствах или персональных компьютерах, позволяют авторизоваться в учетной записи и пройти 2FA[17], извлекать информацию из нескольких десятков облачных хранилищ: Apple, Google, Yandex, iCloud, WhatsApp, Viber, Telegram, расшифровывать резервные копии;

персональные компьютеры: извлечение данных с персональных компьютеров, обнаружение данных учётных записей, токены закладки, истории посещений, файлы куки, Wi-Fi точки доступа, резервные копии iTunes, также позволяет извлекать переписку, медиафайлы и контакты из мессенджеров Viber, Unigram, Skype, Wickr Me, анализировать письма и контакты из почтовых агентов Mozilla Thunderbird, Microsoft Outlook, Microsoft Mail, извлекать данные из веб-браузеров Google Chrome, Mozilla FireFox, Opera, Microsoft Edge, Internet Explorer, получать информацию о системе;

обработка и анализ данных: воссоздание хронологии событий, выстраивание связей между контактами пользователя, установление геолокации, построение маршрутов, выполнение поиска, фильтрации информации по ключевым словам, регулярным выражениям, наборам хешей[18], номерам телефонов, выгрузка настраиваемых отчетов.

Стоит отметить, что крупные корпорации выпуская на рынок новый смартфон или очередное обновление программного обеспечения стараются максимально улучшить защиту этих устройств. Практически все современные устройства оснащены встроенным аппаратным шифрованием, которое более надежно, чем программное, т.к. в нём используются привязанные к устройству

[17] Двухфакторная аутентификация или 2FA - это метод проверки личности пользователя, при котором два из трех возможных факторов аутентификации объединяются для предоставления доступа к веб-сайту или приложению.

[18] Хэш или Хеш-функция (англ. hash function от hash - «превращать в фарш», «мешанина»), или функция свёртки – функция, осуществляющая преобразование массива входных данных произвольной длины в выходную битовую строку установленной длины, выполняемое определённым алгоритмом. Преобразование, производимое хеш-функцией, называется хешированием. Исходные данные называются входным массивом, «ключом» или «сообщением». Результат преобразования называется «хешем», «хеш-кодом», «хеш-суммой», «сводкой сообщения»

аппаратные ключи. Средства «Мобильного криминалиста» позволяют в отдельных случаях обойти данную технологию шифрования для Android-устройств, использующих чипсеты MTK, Qualcomm, Spreadtrum, а также брендов LG и Samsung. Для этого программа модифицирует загрузочный раздел встроенного в гаджет флеш-накопителя или отправляет на устройство модифицированный файл образа загрузчика, открывая таким образом доступ к правам суперпользователя, что позволяет извлечь полный физический образ смартфона либо с извлечением аппаратных ключей, либо с их обходом.

Cellebrite UFED (UFED 4PC) – это универсальный аппаратно-программный комплекс для криминалистических исследований, дающий возможность извлекать, декодировать и анализировать цифровые данные, полученные из мобильных устройств. В состав комплекса входит набор приложений UFED, периферийными устройствами и принадлежностями, нужными для проведения исследований. UFED 4PC может работать как автономно, так и со сторонним программным обеспечением.

UFED 4PC выпускается в вариантах Ultimate и Logical:

UFED 4PC Ultimate включает в себя UFED Physical Analyzer для глубокого декодирования, анализа и подготовки отчетов;

UFED 4PC Logical включает в себя UFED Logical Analyzer для простого декодирования, анализа и подготовки отчетов.

Одним из программных средств является **Belkasoft Evidence Center** – это программное обеспечение для произведения осмотров, компьютерно-технических экспертиз, разработанное специально для правоохранительных органов.

Belkasoft Evidence Center облегчает получение, поиск, анализ, хранение и передачу цифровых улик, находящихся внутри компьютеров и мобильных устройств. Программа быстро извлекает компьютерную информацию из различных источников путем анализа жёстких дисков, образов, облачных приложений, содержимого рабочей памяти, резервных копий iOS, Blackberry и Android, UFED, JTAG и chip-off дампов. Evidence Center автоматически проанализирует источник данных и представит наиболее значительные улики для обзора, подробного изучения или включения в отчёт.

Данный продукт выполняет поиск быстрее, чем большинство других программ, так как Evidence Center не индексирует каждый отдельный файл, находящийся на источнике данных. Вместо этого BEC ищет наиболее значимые в рамках судебно-компьютерной экспертизы типы артефактов. Эффективное использование ресурсов процессора, наряду с кодом, написанным нашей командой профессионалов в области анализа данных, ускоряет обработку дела.

Важно отметить, что указанные программные продукты для осмотра компьютерной техники не модифицируют данные диска или образа, которые подвергаются исследованию.

Специальное программное обеспечение, которое предотвращает все намеренные, неумышленные и системно-инициированные попытки записи на подключенные носители информации. К таким программам относятся:

WriteBlocker или **Innovisijn-Forensiscs USB Write Blocker** – это программное обеспечение, которое работает под управлением операционной системы Microsoft Windows и предотвращает все намеренные, неумышленные и системно-инициированные попытки записи на подключаемые носители информации. В качестве синхронизации с персональным компьютером исследуемых носителей используется адаптеры типа Promise, FireWire, USB, SCSI, многофункциональный кабель Agestar.

Необходимо отдельно отметить программное обеспечение «**Nirsoft**». Прежде всего из-за того, что программный комплекс состоит из комплекса программ, имеющих специфическою сферу применения. С использованием входящих в «Nirsoft» программ можно восстановить пароли, мониторить сеть для просмотра и извлечения cookie, кэша и другой информации, хранимой веб-браузерами, искать по файлам в системе, мониторить изменения в файловой системе и в системном Реестре и многое другое.

Утилиты «**Nirsoft**» пользуются популярностью среди IT- специалистов, системных администраторов. Программы являются бесплатными, не требуют установки. У программ присутствует графический интерфейс, многие программы также поддерживают работу в командной строке. Во время своей работы программы ничего не записывают в реестр Windows, т.е. при использовании с USB носителя не оставляет следов своего присутствия.

Перечень утилит программного комплекса «Nirsoft» достаточно обширен, мы же приведем наиболее используемые утилиты при осмотре:

WinDefThreatsView – это инструмент для Windows 10, который отображает список всех угроз, обнаруженных антивирусом Защитника Windows, и позволяет легко установить действие по умолчанию (Разрешить, Карантин, Очистить, Удалить, Блокировать или Нет действий) для нескольких угроз одновременно.

InstalledPackagesView – это инструмент для Windows, который отображает список всех пакетов программного обеспечения, установленных в системе с помощью установщика Windows, и перечисляет связанные с ними файлы, ключи реестра и сборки .NET. Для каждого установленного программного обеспечения отображается следующая информация: отображаемое имя, отображаемая версия, дата установки, время реестра, расчётный размер, место установки, источник установки, имя файла MSI (в C:\Windows\Installer).

Можно просматривать информацию об установленных пакетах программного обеспечения из локальной системы или из другой системы на внешнем жёстком диске.

Информация об установленном программном обеспечении загружается из следующих ключей реестра:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\Products

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Installer\UserData\Components

Необходимо иметь в виду, что этот инструмент перечисляет только программное обеспечение, установленное установщиком Windows (MSI), он не перечисляет какое-либо программное обеспечение, установленное другими установщиками.

InstalledAppView – это инструмент для Windows 10, который отображает подробную информацию о приложениях Windows 10, установленных в системе. Для каждого приложения Windows отображается следующая информация: имя

приложения, версия приложения, имя реестра, время изменения реестра, папка установки, владелец папки установки, команда удаления.

InstalledAppView позволяет загружать список приложений Windows 10 из локальной системы, удалённого компьютера в сети пользователя и с внешнего диска, подключённого к компьютеру; просматривать XML-файлы приложения Windows (AppxManifest.xml и AppxBlockMap.xml), удалять приложения, открывать установочную папку приложения.

ExifDataView – это утилита, которая считывает и отображает данные Exif, хранящиеся в файлах изображений .jpg, созданных цифровыми камерами. Данные EXIF включают название компании, создавшей камеру, модель камеры, дату и время, когда была сделана фотография, время экспозиции, скорость ISO, информацию GPS (для цифровых камер с GPS).

FullEventLogView – это инструмент для Windows 10/8/7/Vista, который отображает в таблице сведения обо всех событиях из журналов событий Windows, включая описание события. Позволяет просматривать события локального компьютера, события удалённого компьютера в сети, а также события, хранящиеся в файлах .evtx. Он также позволяет экспортировать список событий в файл форматы текст/csv/с TAB разделителями/html/xml из графического интерфейса пользователя и из командной строки.

BrowsingHistoryView считывает и показывает информацию о посещённых сайтах для всех популярных браузеров. Кроме адреса посещённых страниц, показывается её имя, время посещения, счётчик визитов и прочее. Можно извлечь информацию из всех профилей пользователей системы, а также из внешнего диска.

MyLastSearch сканирует кэш и файлы историй веб-браузера и определяет все пользовательские запросы, которые сделаны в самых популярных поисковых системах (Google, Yahoo и MSN), на самых популярных сайтах социальных сетей (Twitter, Facebook, MySpace), а также на других популярных сайтах (YouTube, Wikipedia, Friendster, hi5).

Работа программ IECacheView, MozillaCacheView, ChromeCacheView, MZCacheView напоминает работу BrowsingHistoryView, но просмотр кэша

позволяет видеть каждый индивидуальный файл (скаченные ссылки, изображения и т.д.), а не только адреса посещённых страниц.

Программа ***WebBrowserPassView*** восстанавливает сохранённые пароли из браузеров. Поддерживаются следующие веб-браузеры: Internet Explorer (версии 4.0 - 11.0), Mozilla Firefox (все версии), Google Chrome, Safari и Opera.

Этот инструмент может использоваться для восстановления потерянных/забытых паролей от любого веб-сайта, включая такие популярные веб-сайты как Facebook, Yahoo, Google и GMail.

WirelessKeyView восстанавливает пароли беспроводных сетей (WEP/WPA), хранимые на компьютере, работая на всех версиях Windows.

SmartSniff – это утилита сетевого мониторинга, которая позволяет захватывать TCP/IP пакеты, которые проходят через сетевой адаптер и просматривать захваченные данные как последовательность разговоров между клиентами и серверами. Можно просматривать TCP/IP беседы в режиме Ascii (для протоколов на основе текста, таких HTTP, SMTP, POP3 и FTP.) или как шестнадцатеричный дамп (для нетекстовых протоколов, таких как DNS).

Wireless Network Watcher – это программа, которая сканирует беспроводную сеть и отображает список всех компьютеров и устройств, которые в данный момент подключены к ней. Для каждого компьютера или устройства, подключённого к сети, отображается следующая информация: IP адрес, MAC адрес, компания-производитель сетевой карты и, опционально, имя компьютера.

WifiHistoryView программа для Windows 10/8/7/Vista, которая отображает подключения к беспроводным сетям на вашем компьютере. Для каждого события, когда компьютер подключился или отключился к/от беспроводной сети, отображается следующая информация: дата/время когда произошло событие, имя сети (SSID), имя профиля, имя сетевого адаптера, BSSID роутера/точки доступа и другая.

DomainHostingView – это программа для Windows, которая собирает обширную информацию о домене, используя серию DNS и WHOIS запросов и генерирует HTML отчёт, который можно открыть в веб-браузере. Информация включает в себя: хостинг-компанию или дата центр, который хостит веб-сервер,

почтовый сервер и сервер доменных имён (DNS) указанного домена, даты создания/изменения/истечения домена, владельца домена, регистратора домена, список всех DNS записей и другое.

IPNetInfo –позволяет найти всю доступную информацию об IP адресе: владельца IP адреса, страну/штат, диапазон IP адресов, контактную информацию (адрес, телефон и email) и другое. IPNetInfo может извлекать все IP адреса из заголовков сообщения электронной почты – достаточно скопировать их в программу и она отобразит всю информацию об этих IP адресах.

WhoisThisDomain получает информацию о зарегистрированных доменах. Она автоматически подключается к правильному WHOIS серверу, в соответствии с доменом первого уровня, и получает WHOIS записи этого домена.

MACAddressView делает поиск по базе данных MAC адресов для поиска информации о компании (имя компании, адрес, страна), которая произвела данное сетевое устройство.

MobileFileSearch – это инструмент для Windows, который позволяет искать файлы внутри мобильного устройства (смартфона или планшета), подключённого к USB-порту компьютера, с помощью протокола передачи мультимедиа (MTP). Можно искать файлы по их размеру, времени создания, времени изменения или имени (используя подстановочный знак). MobileFileSearch также позволяет активировать поиск из командной строки и затем экспортировать результат в файл или копировать найденные файлы в нужную папку на вашем компьютере.

FileActivityWatch – это инструмент для Windows, который отображает информацию о каждой операции чтения/записи/удаления файлов, происходящей в системе. Для каждого файла FileActivityWatch отображает количество байтов чтения/записи, количество операций чтения/записи/удаления, первую и последнюю временную метку чтения/записи, а также имя/идентификатор процесса, ответственного за операцию с файлом.