Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ
УНИВЕРСИСТЕТ»

В. В. Подтопельный

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие по выполнению практических работ
для студентов специальности 10.05.03 " Информационная безопасность
автоматизированных систем ", специализация «Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2022

Рецензент

Доцент кафедры информационной безопасности института информационных технологий ФГБОУ ВО «Калининградский государственный технический университет» А. Г. Жестовский.

Подтопельный, В. В.
Аудит информационной безопасности: учебно-методическое пособие по выполнению практических работ для студентов специальности 10.05.03 "Информационная безопасность автоматизированных систем ", специализация «Безопасность открытых информационных систем». – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 59 с.

Учебное пособие включает в себя рассмотрение практических вопросов в области защиты информации по дисциплине «Аудит информационной безопасности». Представлены методические указания по выполнению практических работ в соответствии с тематическим планом дисциплины.

Пособие предназначено для студентов 5 (семестр А) курсов специальности 10.05.03 «Информационная безопасность автоматизированных систем» и смежных специальностей.

Рис. – 30, табл. - 4, список лит. – 21 наименований

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала кафедрой информационной безопасности 19 мая 2022 г., протокол № 7

Учебно-методическое пособие по выполнению работ рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий ФГБОУ ВО «Калининградский государственный технический университет» от 28 июня 2022 г., протокол № 4

ОГЛАВЛЕНИЕ

Введение

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 " Информационная безопасность автоматизированных систем ", специализация «Безопасность открытых информационных систем», изучающих дисциплину «**Аудит информационной безопасности».**

Цель изучения практического курса дисциплины обучить студентов выявлять и анализировать угрозы и уязвимости инфраструктур цифрового типа на предприятиях, определять особенности поведения злоумышленников в распределенных системах обработки информации**.**

Для успешного освоения лабораторного курса дисциплины, в соответствии с учебным планом, ей предшествуют **«Безопасность вычислительных сетей», «Безопасность систем баз данных», «Безопасность операционных систем», «Правовое обеспечение информационной безопасности»**.

Далее в пособии представлен набор лабораторных/практических работ. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение лабораторного курса дисциплины, возможно, вам потребует больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе УМП дисциплины «Балльно-рейтинговая система» приведен порядок применения балльно-рейтинговой системы контроля успеваемости.

В результате выполнения лабораторных работ ожидается, что студенты сформируют навыки применения:

- выявлять возможные способы нарушения информационной безопасности при работе

автоматизированных систем обработки информации и определять их специфику;

- в рамках задач обеспечения информационной безопасности решать вопросы использования радиоэлектронной аппаратуры и других технических средств;

- используя современные методы и средства разрабатывать и оценивать модели и политику безопасности;

- определять специфику реализации системы зашиты информации в автоматизированных системах в соответствии со стандартами по оценке защищенных систем;

- используя формальные методы, давать оценку качества предлагаемых решений защиты программ и данных программно-аппаратными средствами;

- применять системный подход к обеспечению информационной безопасности в различных сферах деятельности, включая комплекс технических и организационных мер, учитывающих особенности функционирования предприятия и решаемых им задач;

- разрабатывать проектные решения и реализовывать комплексную систему защиты информации, оценивать ее качество.

Помимо данного пособия студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделу ЭИОС, в которые более оперативно вносятся изменения для адаптации лабораторного курса дисциплины под конкретную группу.

Программное обеспечение

1. Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения (Microsoft Office), по соглашению V9002148 Open Value Subscription (срок действия: три года)

2. Программное обеспечение, распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU, по которой автор передаёт программное обеспечение в общественную собственность):

– Snort (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом);

– Ethereal (Программы перехвата и анализа сетевых пакетов);

– NMAP(Программа сканирование сетевых ресурсов);

– MySQL (Система управления базами данных).

Типовое ПО на всех ПК:

1. Microsoft Desktop Education (операционные системы Microsoft Windows Desktop operating system, офисные приложения Microsoft Office, по соглашению V9002148 Open Value Subscription). Дата заключения контракта 05.07.2018. Номер контракта 0335100016118000073-0484577-02.

2. Антивирусное программное обеспечение Kaspersky Total Space Security Russian Edition, лицензия 17EO-171225-104659-470-270, срок использования с 2017-12-26 до 2020-03-13

Специализированное ПО:

1. VMWare Workstation, Страж-NT, Панцирь-К (по государственному контракту №10/13А от 19 апреля 2013 года), (на 2 компьютера – Vmware License Purchase Information № 22033811ОВ);

Open Value Subscription;

Практическая работа № 1. Защищенность системы с точки зрения риска

Программно-аппаратные средства: стандартные средства Microsoft Office.

1.Теоретический материал

При аудите организации требуется подготовить:

- описание функциональных обязанностей и структурные подчинения сегментов и специалистов ИБ в организации;
- документы, о внедрении политики информационной безопасности (в том числе документированного подхода к оцениванию и управлению рисками в рамках всей компании);
- документация на процессы обслуживания и администрирования информационной системы;
- документация по управлению рисками и результаты оценки рисков;
- документация по подготовке периодических проверок по оцениванию и управлению рисками;
- документация по системе управления ИБ;
- перечень средств управления безопасностью в документе «Ведомость соответствия»;
- описание контрмер для противодействия выявленным рискам.
- все перечисленные проверки выполняются с использованием принятых в компании подходов к оценке и управлению рисками.

При **аудите информационной системы** предварительно рассматривается:

- политика информационной безопасности предприятия;
- документацию по проведенному оцениванию рисков;
- документацию по средствам управления ИБ;
- эффективность средств защиты информации.

Этапы проведения аудита [1, 2]:

Этап первый. Подготовка к аудиту:

- определение объекта аудита;
- выбор критериев и методов аудита;
- выбор средств и способов аудита;
- формирование команды аудиторов;
- определение объема и масштаба аудита, установление его сроков.

Этап второй. Проведение процедуры аудита:

- анализ состояния ИБ объекта аудита;
- инвентаризация, регистрация, сбор и проверка состояния компонентов объекта;
- сбор статистических данных и результатов инструментальных измерений уязвимостей и угроз;

- оценка результатов проверки, системы управления, связи и безопасности.

- формирование отчета (покомпонентное) по итогам аудита (в зависимости от сегментации объектов аудита);

объекта аудита и различным аспектам ИБ.

Этап третий. Анализ результатов аудита:

- составление итогового отчета;

- формирование рекомендаций по комплексу мер, направленных на повышение эффективности существующей системы защиты;

- разработка плана мероприятий по устранению уязвимостей и недостатков в обеспечении ИБ.

На **подготовительном этапе** определяется порядок работ, последовательность реализации работ, ресурсы, требуемые для работ. Сформированный план работ согласовывается с заказчиком. На этом этапе производится следующее:

- назначение и цели предстоящего аудита, порядок их достижения, границы аудита.

- функции, структура и состав корпоративной системы, потенциальные уязвимости в системе управления информационной безопасностью.

- способы оценки квалификации специалистов и сотрудников службы ИБ;

- способы категорирования информации;

- методы и инструментарии оценки временных затрат и затрат ресурсов компании на аудит информационной безопасности;

- состав группы экспертов в области безопасности корпоративных систем и распределение обязанностей между ними;

- параметры корпоративной информационной сети предприятия и среды ее функционирования, оказывающие существенное влияние на качество аудита безопасности;

- совокупность учитываемых при проведении аудита безопасности требований международных, государственных, межведомственных и внутренних стандартов;

- внутренняя отчетная документация, оформление и при необходимости корректировка концепции и политики информационной безопасности предприятия;

- согласованный с заказчиком общий порядок проведения аудита безопасности компании может быть отражен в соответствующем техническом задании.

2. **Этап анализа требований и исходных данных** составляет главную часть планирования аудита. В процессе анализа рассматриваются:

– *требования информационной безопасности.* Цель аудита – объективно и оперативно оценить и проверить соответствие исследуемой

корпоративной системы защиты компании предъявляемым к ней требованиям ИБ. Поэтому для такой оценки необходимо сначала рассмотреть требования информационной безопасности. Основными требованиями информационной безопасности для отечественных предприятий и компаний являются требования руководящих документов Гостехкомиссии РФ, законов Российской Федерации, внутриведомственных, межведомственных, национальных и международных стандартов. Кроме этого, для каждой корпоративной информационной системы необходимо учитывать специальные требования внутреннего использования, согласованные с концепцией и политикой безопасности компании.

– *исходные данные для проведения аудита.* В руководящем документе Гостехкомиссии «Положение по аттестации объектов информатизации по требованиям безопасности информации» приводится стандартный перечень исходных данных, необходимых для разработки программы и методики аттестационных испытаний. Помимо стандартных исходных данных могут использоваться и дополнительные исходные данные, специфичные для каждого конкретного предприятия, например, статистика нарушений политики безопасности компании, статистика внешних и внутренних атак, уязвимости наиболее критичных корпоративных информационных ресурсов и т. д. Также нужно учитывать, что, как правило, руководство компании имеет собственные взгляды на информацию, предоставляемую в качестве исходных данных для аудита безопасности. Поэтому между заказчиком и исполнителем работ по аудиту ИБ рекомендуется заключить специальное соглашение о конфиденциальности или соответствующий протокол о намерениях.

– *границы проведения аудита.* При определении рамок проведения аудита необходимо в равной степени учитывать организационный, технологический, и программно-технический уровни обеспечения информационной безопасности. В противном случае результаты аудита не будут объективно отражать реальный уровень информационной безопасности компании. Например, дорогостоящие аппаратно-программные средства защиты информации могут оказаться бесполезными, если неправильно определены и реализованы меры и мероприятия на организационном и технологическом уровнях. При определении рамок аудита необходимо зафиксировать штатные условия функционирования корпоративной информационной системы безопасности предприятия.

– *области детального изучения.* При проведении аудита основное внимание должно уделяться компонентам и подсистемам, осуществляющим обработку конфиденциальной информации предприятия. При этом необходимо уметь рассчитать возможный ущерб, который может быть нанесен компании в случае разглашения конфиденциальной информации и

нарушения политики безопасности. Это должно быть отражено в соответствующих документах компании, регламентирующих ее политику информационной безопасности. Для определения возможного ущерба могут использоваться разнообразные формальные методы, например методы экспертных оценок.

– *требуемый уровень детализации и полноты.* В большинстве случаев для получения адекватных результатов достаточно провести базовый анализ корпоративной системы защиты информации, позволяющий определить общий уровень ИБ предприятия и проверить его на соответствие некоторым требованиям безопасности. В некоторых случаях дополнительно требуется провести детальный анализ, цель которого – количественно оценить уровень информационной безопасности компании на основе специальных количественных метрик и мер информационной безопасности. Для этого сначала определяются все необходимые количественные показатели, а затем производится оценка уровня информационной безопасности компании. Существенно, что при этом становится возможным сравнивать уровень безопасности компании с некоторым эталоном, определять тенденции и перспективы развития системы корпоративной безопасности, необходимые инвестиции и т. д.

3. На ***этапе расчета трудоемкости и стоимости*** проводимых работ по данным проведенного анализа оцениваются временные, финансовые, технические, информационные и прочие ресурсы, необходимые для аудита информационной безопасности. Выделение ресурсов рекомендуется производить с учетом возможных нештатных ситуаций, способных увеличить трудоемкость аудита безопасности.

4. Завершается планирование аудита ***этапом формализации и документирования выполнения аудита,*** что, прежде всего, подразумевает подготовку и согласование плана проведения аудита. План проведения аудита в общем случае включает в себя следующие разделы:

- ***краткая характеристика работ***. Здесь представляются все необходимые сведения о порядке проведения работ;
- ***введение.*** Указывается актуальность проведения аудита безопасности, особенности и требования к порядку проведения аудита, характеристика исследуемого объекта, рамки проведения аудита, общий порядок работ, требования по фиксации результатов аудита. Дополнительно приводятся сведения о категорировании корпоративной информации, например конфиденциальной и строго конфиденциальной. Также перечисляются основные решаемые задачи, ограничения, выполняемые функции и критерии оценивания уровня ИБ предприятия, требования нормативных документов РФ, международных стандартов и внутренних требований предприятия;
- ***распределение обязанностей***. Определяется штат и функциональные обязанности группы специалистов, которые будут

проводить аудит безопасности;

- ***требования информационной безопасности***. Фиксируется обоснованный выбор требований ИБ, определяются критерии и показатели оценки ИБ предприятия, выбираются количественные метрики и меры безопасности. Помимо нормативной и законодательной базы РФ дополнительно рекомендуется использовать требования международных и внутренних стандартов компании, актуальные для каждой отдельно взятой.

- ***формализация оценок уровня безопасности предприятия.*** Определяются качественные и количественные параметры для получения объективных оценок уровня ИБ предприятия. Перечисляются задачи, выполняемые при проведении базового и детального анализа информационных рисков. В этом разделе отражаются критичные информационные ресурсы компании, оценка экономической эффективности ее деятельности, используемые модели, методы средства проведения аудита безопасности, исходные данные.

- ***план-график работ***. Определяются сроки, календарный план выполняемых работ, время их окончания, формы отчетных документов, требования по приему-сдаче работы и прочее;

- ***поддержка и сопровождение***. Перечисляются требования к административной, технологической и технической поддержке аудита ИБ;

- ***отчетные документы***. Основными отчетными документами являются отчет по результатам аудита безопасности, концепция и Политика информационной безопасности, План защиты компании;

- ***приложения***. В приложениях приводятся протоколы проверок, а также информация по методикам и инструментарии проведения аудита, выявленные замечания, рекомендации и прочее.

Исходя из опыта многих компаний, занимающихся проведением аудита информационной безопасности, может быть рекомендован следующий алгоритм его проведения.

I. ***Определение и систематизация перечня угроз информационной безопасности***.

1. Оформление официальных запросов предоставления информации об организационно-штатной структуре, организации сети, организации защиты информации, отправка Заказчику.

2. Получение информации, проведение первичного анализа системы информационной безопасности объекта, выбор инструментальных средств для проведения исследования уязвимостей сети.

3. Выезд на предприятие для предварительного обследования корпоративной сети:

- проведение экспресс-анализа по выделению наиболее критичных автоматизированных систем, исходя из потенциальной ценности, обрабатываемой и хранимой в них информации;

- проведение работы по построению структурной и функциональной схемы информационной системы с обозначением основных информационных потоков обмена информацией;
- проведение работы по построению типовой модели нарушителя для информационной системы, перечня угроз информационной безопасности в информационной системе (совместно с представителями структурных подразделений безопасности);
- проведение работы по наложению перечня сведений ограниченного распространения на функциональную схему информационной системы, выделение критичных информационных ресурсов, методов и средств их защиты;
- проведение работы по изучению организационного обеспечения информационной безопасности в части организационно-штатной структуры, правового и технологического обеспечения;
- проведение работы по анализу уязвимостей компьютерной сети, в том числе с помощью инструментальных средств;
- проведение работы по анализу рисков в информационной системе, выработка уровней риска по различным видам угроз для конкретных информационных ресурсов корпоративной сети объекта;
- формирование выводов;
- проведение согласования отчетной документации по первому этапу работ.

II. Разработка концепции обеспечения информационной безопасности и эскизного проекта

1. Определение комплексных критериев для построения системы информационной безопасности – установление приемлемых уровней риска (совместно со службой безопасности).

2. Разработка концепции обеспечения информационной безопасности заказчика, включающей:

- описание целей защиты информации;
- описание задач, решаемых для достижения целей защиты информации;
- описание основных объектов защиты, угроз их безопасности, учитывая специфику деятельности;
- взгляды на основные направления, условия и порядок практического решения задач информационной безопасности по направлениям: правовому, организационному и техническому;
- основные принципы взаимодействия подразделений для наиболее эффективного достижения целей системы информационной безопасности;
- перспективную программу создания системы информационной безопасности.

3. Разработка требований к системе ИБ, включающих:

- общие принципы защиты информационного ресурса, классифицированные в соответствии с угрозами информационной безопасности;
- требования к организационному и правовому обеспечению информационной безопасности с учетом выбранного критерия;
- описание конкретных мер защиты, рекомендованных для построения системы информационной безопасности с учетом выбранного критерия;
- требования к настройкам используемого в информационной системе активного сетевого оборудования, операционных систем, систем управления базами данных, почтовых систем и Web-браузеров, реализации заложенных в них механизмов безопасности, обновлению программного обеспечения, установке необходимых обновлений программного обеспечения;
- описание требований к средствам защиты информации в корпоративной сети, включая централизованные системы управления защитой сети, интегрированные системы безопасности с системами управления сетью, распределенные межсетевые экраны, системы виртуальных частных сетей, системы аудита и мониторинга безопасности сети, системы централизованной антивирусной защиты, средства обеспечения защиты рабочих станций от несанкционированного доступа, системы электронной цифровой подписи, системы поддержания отказоустойчивости;
- требования по настройке элементов системы защиты.

4. Проведение технико-экономической оценки мероприятий по обеспечению информационной безопасности.

5. Разработка Эскизного проекта обеспечения безопасности на объекте Заказчика.

6. Разработка организационно-распорядительной документации согласно заданию Заказчика, а также на основании результатов проведенного исследования.

7. Разработка Плана защиты, включающего календарный план построения системы информационной безопасности.

8. Предложения по управлению (оценка и переоценка рисков предприятия) информационной безопасностью предприятия.

9. Предложения по сопровождению корпоративной системы обеспечения безопасности.

Приведем примерный план по проведению аудита информационной безопасности с указанием времени выполнения его основных этапов.

2. Практическая часть

2.1 Изучить основной теоретический материал лабораторной работы.

2.2 Придумать или использовать реальную ИС некоторой организации.

2.3 Внести структурную схему и описание вашей ИС в отчет.

2.4 Составить и внести в отчет перечни типов угроз ИБ и информационные ресурсы, присутствующие в данной ИС.

Контрольные вопросы:

1. Дайте определения безопасности информации, уязвимости информации, защищенности информации, угрозам безопасности информации, защите информации. Перечислите источники угроз безопасности информации.
2. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
3. Поясните суть методики оценки уязвимости информации.

Практическая работа № 2. Последовательность осуществления инвентаризации инфраструктуры организации

Цель работы: изучение порядка активного аудита информационной безопасности компьютерных систем.

Программное обеспечение: ОС Microsoft Windows XP/2003/ 2008R2/Vista/7/8/8.1/2012/2012R2, ОС Kali Linux, hping3, nmap, ScanOval.

1.Теоретический материал

Последовательность осуществления инвентаризации инфраструктуры организации.

Перед проведением аудита необходимо собрать все необходимые сведения об организации.

Список данных, которые необходимы для проведения аудита, следующий:

1. Общие сведения об организации:

– иерархическая структура организации;

– информация об уровне конфиденциальности данных, которые хранятся, обрабатываются и передаются по каналам связи с использованием компьютерных технологий;

– руководящие документы по хранению, обработке и передаче информации;

– положения о защите информации;

– список информации, составляющей коммерческую или служебную тайну в организации;

2. Информация, относящаяся к технологическому характеру о функционировании организации заказчика:

– технологические связи на уровне передачи файлов или потоков данных;

– направления потоков данных;

– инструкции для сотрудников;

– доступ к критичным средствам: информации, администраторам безопасности;

– планы сервисных и эксплуатационных мероприятий;

– распределение критически важных для организации процессов обработки и передачи данных;

– проекты по развитию и совершенствованию ИС;

– информация о расположении критических участков и мест хранения ценностей, данных;

– информация о контроле и управлении доступа в критичных участках.

3. Вся информация об имеющихся средствах вычислительной техники (СВТ).

Серверные платформы:

– количество серверов;

– тип ОС, версия ОС (patch, service pack);

– сетевые протоколы;

– технологическая документация;

– использование средств защиты информации, возможность архивирования;

– документация производителей СВТ.

4. Информация о сетевых соединениях и топологии сети:

– карта сети;

– локализация компонентов сети, наличие на них критичной информации;

– распределение рабочих станций;

– используемые Internet-сервисы;

– организация выхода в Internet;

– доступ с WWW-узла к системам электронного документооборота;

– типы сетевого оборудования, версии прошивок и ОС коммутаторов, их особенности;

– системное сетевое ПО;

– типы применяемого сетевого оборудования, версии прошивок/ОС маршрутизаторов, коммутаторов, параметры настроек;

– проекты развития ИС организации;

5. Информация об используемых клиентских рабочих местах:

– тип, количество и место установки;

– аппаратные платформы, описание, фирма-поставщик, аппаратное обеспечение;

– ОС, полная ее версия, наименование, полная версия «заплат» (patch);

– использование приобретенных средств защиты от несанкционированного доступа (НСД).

6. Информация о ПО:

– перечень особых систем (управление базой данных);

– перечень прикладного ПО, ассоциированного с серверами и клиентскими рабочими местами;

– решаемые задачи ПО;

– производитель;

– ОС, полная ее версия, наименование, полная версия «заплат» (patch);

– сертификаты производителя;

– специальные возможности ПО;

– наличие критичных процессов передачи данных и электронной обработки для организации.

7. Информация по конкретным системам, поддерживающих и контролирующих работу ИС:

– средства архивирования, их места и режим работы;

– система протоколирования действий пользователя;

– средства аутентификации, авторизации, системного аудита.

8. Общие сведения о работе ИС:

– наличие администратора сети;

– наличие администратора безопасности сети;

– порядок распределения прав доступа к критическим ресурсам;

– правила резервного копирования и восстановления важной информации;

– управление работой в критических ситуациях.

9. Данные о важности источников информации по отношению к технологиям организации.

10. Информация о средствах защиты ИБ.

11. Информация о существующих технических средствах защиты информации:

– межсетевые экраны;

– сертификаты производителей;

– схема установки;

– полная версия «заплат» (patch);

– системы мониторинга безопасности;

– криптографические средства;

– средства предотвращения НСД;

– системы аудита ИБ;

– анализаторы трафика.

Порядок применения механизмов сбора информации следующий:

– сетевые сканеры (Nmap, Netcat);

– установление маршрутов доступа, особенностей доступа инфраструктуры (Nmap, IVRE);

– определение уровня защищенности благодаря тестирующим программам (Nmap, Nessus, SSS) [13];

– определение сервиса сетевого доступа с целью подключения к службам ИС.

На данном этапе осуществляется проверка уязвимостей удаленного хоста и возможность подключения сторонних пользователей.

При осуществлении второго этапа необходимо установить систему удаленного доступа на основе протоколов VNC или использовать ее аналоговую службу. Появится возможность получать доступ к ОС АРМ и выполнять локальное сканирование с использованием, например, такой программы, как ScanOVAL.

Так можно получить достоверные сведения о ПО пользователя и инфраструктурной среде узла сети. Из-за того, что рабочее место пользователя может периодически изменяться из-за отсутствия или нестабильности политики безопасности, при осуществлении сканирования необходимо сосредоточиться на безопасности сетевых служб, которые необходимы для взаимодействия со службами КИС организации.

В результате анализа выявлены различия в характере информации о состоянии безопасности узлов сети, собираемых при инструментальном исследовании объекта [5]. Тем не менее фактор гарантии доступности и достоверность информации (перечисленных в Табл. 2) были приняты во внимание. Порядок предоставленной информации указывает нужный порядок сбора данных при обнаружении сетевых узлов.

Подбор инструментов, необходимых для проведения удаленного аудита. Для проведения удаленного аудита необходимо получить всю нужную информацию об удаленном АРМ заказчика. В данной работе будет использоваться ПО Oracle VM VirtualBox с двумя установленными виртуальными ОС Microsoft Windows 7. Одна ОС будет считаться нашим рабочим местом, другая – удаленное АРМ заказчика (рисунок 1).

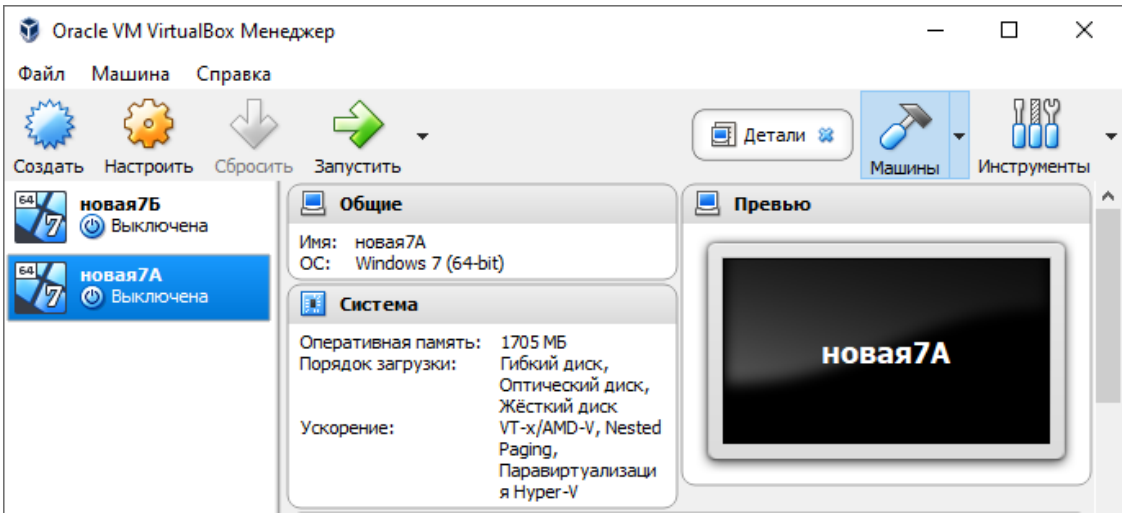


Рисунок 1. Практическая установка

На начальном этапе для получения информации используется программа Nmap. Nmap – это инструмент сканирования сети. С помощью его можно получить информацию о различных параметрах сканируемого компьютера. Также можно узнать открытые порты, установленную ОС, различные сервисы, которые запущены на хосте и многое другое. Также можно выполнять специальные скрипты, позволяющие выявлять уязвимости в конкретном ПО.

Запуск программы Nmap осуществляется из командной строки. При введении команды nmap –h выводится перечень всевозможных команд с пояснением, которые можно использовать как вместе, так и по отдельности (рисунок 2).

```
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Настя>nmap -h
Nmap 7.91 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] <target specification>
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
```

Рисунок 2. Перечень всевозможных команд

Результатом работы программы является список отсканированных портов удаленной машины с обозначением номера и состояния порта, типа использованного протокола и так далее.

Для того, чтобы получить информацию об удаленном АРМ, необходимо узнать его IP-адрес. Для этого на второй виртуальной машине в командной строке необходимо ввести команду ipconfig для получения IP-адреса (рисунок 3).

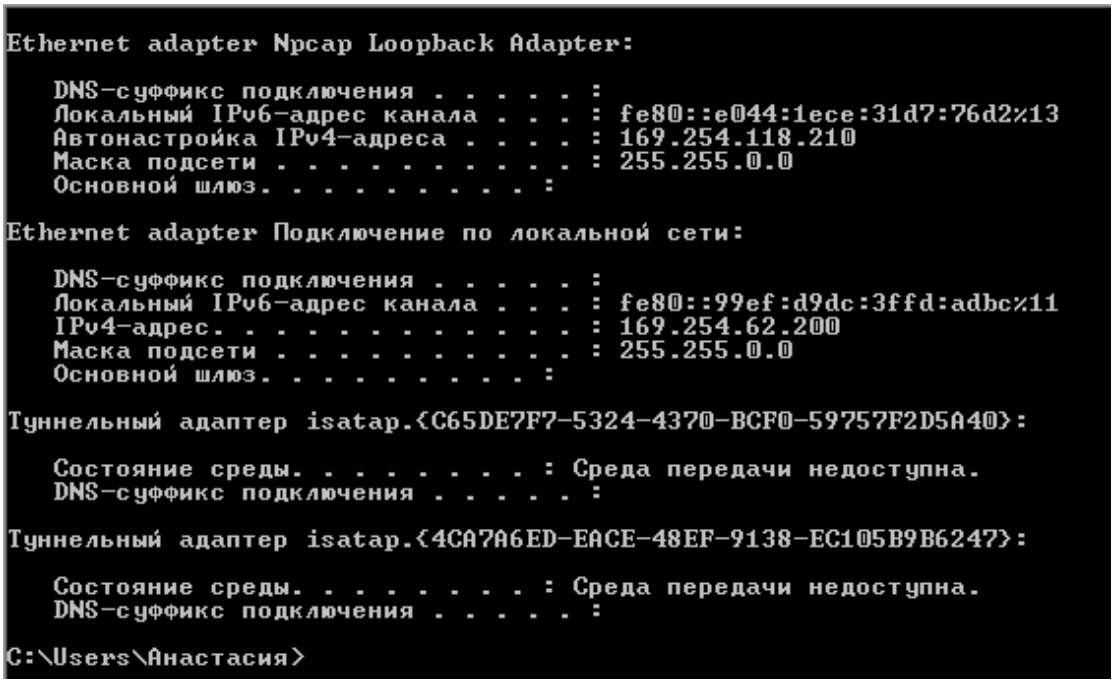


Рисунок 3. Получение IP-адреса

В данном случае IP-адрес удаленного АРМ 169.254.62.200, а маска подсети – 255.255.0.0. Далее можем произвести Ping сканирование с помощью команды ping 169.254.162.200 (Рисунок 4).

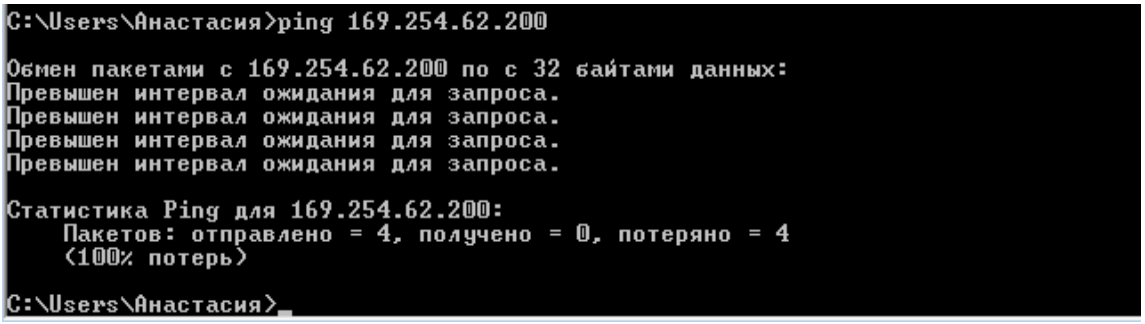


Рисунок 1. Попытка произвести Ping сканирование

Данная команда является простым средством для проверки доступности удаленного узла. Она работает на протоколе ICMP (Internet Control Message Protocol), который, в свою очередь, осуществляет работу на сетевом уровне модели стека протоколов TCP/IP. Как видно на рисунке, пакеты потеряны, нарушена маршрутизация с удаленным АРМ. Для решения такой проблемы на удаленном АРМ можно отключить брандмауэр либо на обеих ОС в центре управления сетями включить сетевое обнаружение, лучше все-таки воспользоваться вторым вариантом. Далее еще раз произвели Ping сканирование (рисунок 5).

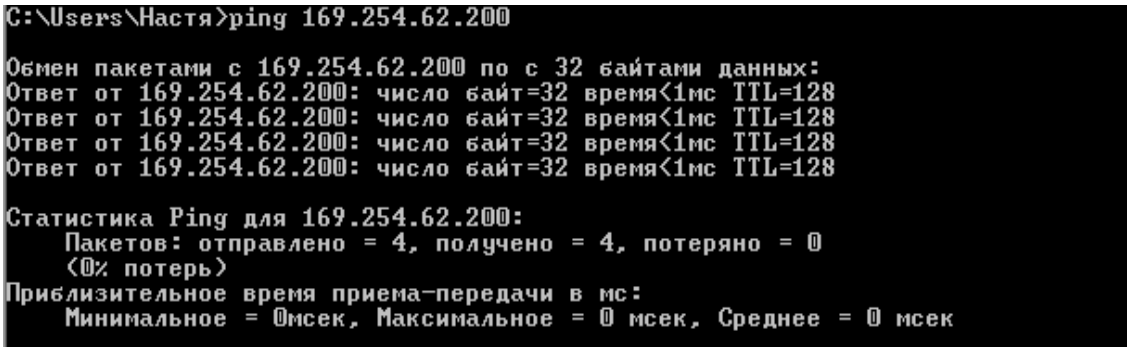


Рисунок 5. Повторная попытка Ping сканирования

В конечном итоге удалось произвести Ping сканирование благодаря отключению брандмауэра. По умолчанию команда задает размер данных ICMP сообщения, которые равны 32 байтам, абсолютно все запросы упаковываются в IP-пакет, у которых присутствует поле TTL (time to live), а по умолчанию команда ping присваивает полю значение 128. Также можно увидеть общую представленную информацию: было отправлено и получено по 4 пакета, а утеряно 0. Время прохождения пакетов по сети: максимальное, минимальное и среднее было равно 0.

Зная IP-адрес удаленного АРМ, можно получить список открытых портов с помощью такой команды как nmap 169.254.62.200 (рисунок 6) [12].

Рисунок 6. Список открытых портов

Существует шесть основных состояний портов:

– состояние 1 – открыт (open) – приложение получает пакеты или запросы на соединение через порт;

– состояние 2 – закрыт (close) – порт может отвечать на запросы, но при этом не будет пользоваться приложением;

– состояние 3 – фильтруется (filtered) – запросы не могут дойти до порта, следовательно, невозможно понять закрыт он или открыт;

– состояние 4 – не фильтруется (unfiltered) – порт считается доступным, но у Nmap нет возможности определить закрыт он или нет;

– состояние 5 – открыт|фильтруется (open|filtered) – в данном случае нельзя понять фильтруется порт или открыт;

– состояние 6 – закрыт|фильтруется (close|filtered) – в таком случае невозможно определить фильтруется или закрыт.

В нашем случае все порты открыты.

Возможен такой вариант, что у заказчика по городу существует несколько филиалов и потребуется произвести сканирование всех этих точек. Можно реализовать активное сканирование с использованием IVRE всех IP, которые находятся, например, в Калининграде. IVRE – фреймворк разведки сетей.

Для получения всех IP-адресов, которые находятся в нашем городе, необходимо скачать его базу данных (рисунок 7).

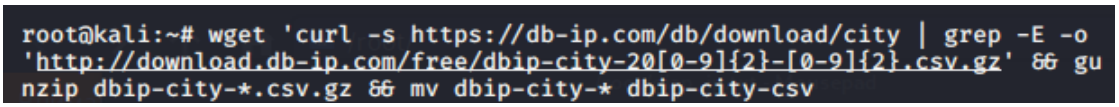


Рисунок 7. Скачивание базы данных

Далее необходимо составить список IP нашего города (рисунок 8).

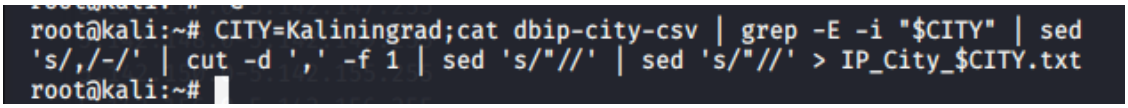


Рисунок 8. Создание списка IP в документ IP_City_$CITY.txt

Этот список в документе будет выглядеть следующим образом (рисунок 9):

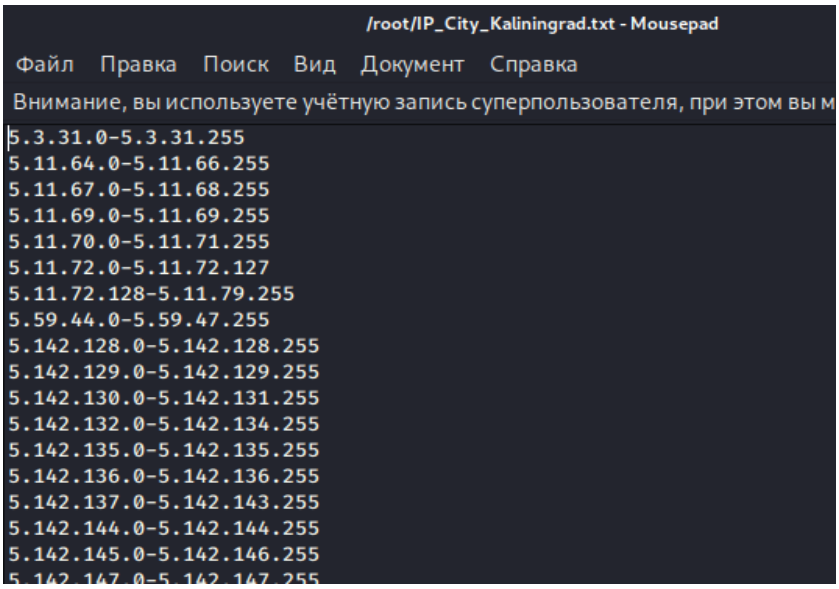


Рисунок 9. Вывод списка в документе

Далее после получения всего перечня IP-адресов можно осуществить поиск необходимого нам IP-адреса, который предоставил сам заказчик, и узнать состояние порта, и если он будет открыт, то это значит, что удаленное АРМ получает пакеты или запросы на соединение через порт. Следовательно, можно узнать некоторую информацию об этом IP-адресе. Этот инструмент позволит проводить подробное сканирование через глобальную сеть. Он схож с Nmap, но у него существует больше функций и есть возможность получить больше информации в условиях отсутствия канала VPN или другого прямого соединения.

Далее можно определить версию ОС. Для этого потребуется такая команда, как nmap – O 169.254.62.200 (рисунок 10) [12].

Рисунок 2. Определение ОС

С помощью вышеупомянутой команды удалось узнать ОС и ее версию, информацию о службах, а также был выявлен список открытых портов.

Этой информации будет достаточно, чтоб злоумышленник смог найти уязвимости в ОС.

Еще можно воспользоваться командой nmap –sV 169.254.62.200, которая сможет определить версии программ, запущенные на удаленном АРМ (рисунок 11) [12].

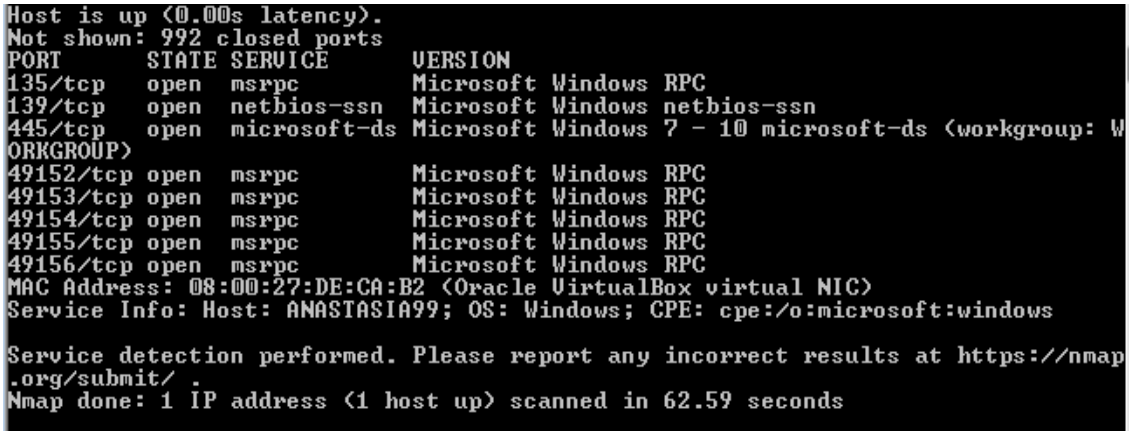


Рисунок 3. Определение версии программы

Интересной особенностью программы Nmap является возможность использования скриптов Nmap Scripting Engine (NSE) (скриптовый движок Nmap). Помимо обычной проверки портов с помощью Nmap можно задействовать и NSE, который позволит получить более углубленную и расширенную информацию о всех процессах.

В поддиректории каталога Nmap находится папка scripts, а в ней существует 598 скриптов NSE. Все скрипты сгруппированы в разные категории в зависимости от использования.

Например, можно с помощью команды nmap –sV –script=vulscan-master/vulcan.nse 169.254.62.200 осуществить сканирование на основе скриптов, где будут выявлены уязвимости удаленного АРМ.

Итак, использование программы Nmap позволило получить некоторую информацию, необходимую для проведения аудита. Но, к сожалению, всей этой информации было недостаточно для полного представления об удаленном АРМ. Поэтому необходимо подключать другие инструменты, которые смогут помочь собрать всю необходимую информацию. Далее можно воспользоваться программой XSpider. XSpider – сканер уязвимостей, который позволит оценить текущее состояние инфраструктуры организации, точно может обнаружить сетевые узлы, покажет всевозможные открытые порты, определяет ОС, серверные приложения, а также есть возможность отследить изменения в состоянии ИС.

На серверах, рабочих станциях, сетевом оборудовании осуществляется поиск уязвимостей, проводится тщательная проверка веб-сайтов. База

уязвимостей постоянно пополняется новыми данными об угрозах. После обнаружения уязвимостей XSpider выдает необходимую информацию, а также детальную информацию и точные рекомендации для их устранения [14].

XSpider можно установить на абсолютно любую ОС Windows [14]. После установки данной программы, на экране появится окно программы. Чтобы начать сканирование хоста, необходимо нажать на кнопку «Добавить хост». После чего в строку ввести нужный IP-адрес. После того как выбран хост, можно перейти в профиль проверки. Был выбран стандартный профиль проверки (рисунок 12).

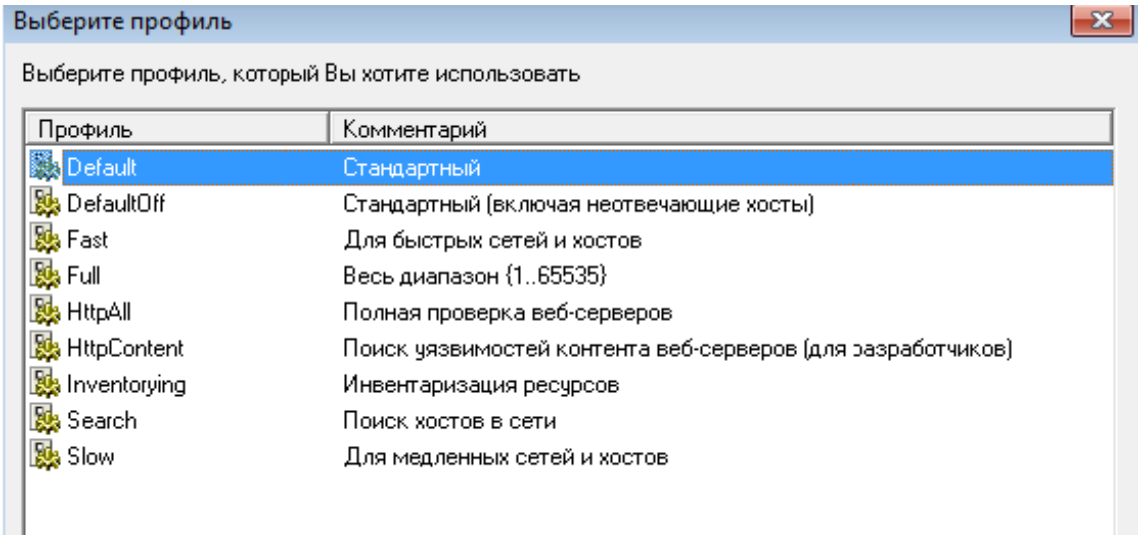


Рисунок 12. Выбор стандартного профиля проверки

Также можно создать индивидуальный профиль, который будет лучшим и удобным. Характеристики выбора будут включать в себя поиск хостов, сканер портов, сканер уязвимостей, идентификация сервисов, определение уязвимостей, анализатор контента и скриптов, авторизация и многое другое (рисунок 13).

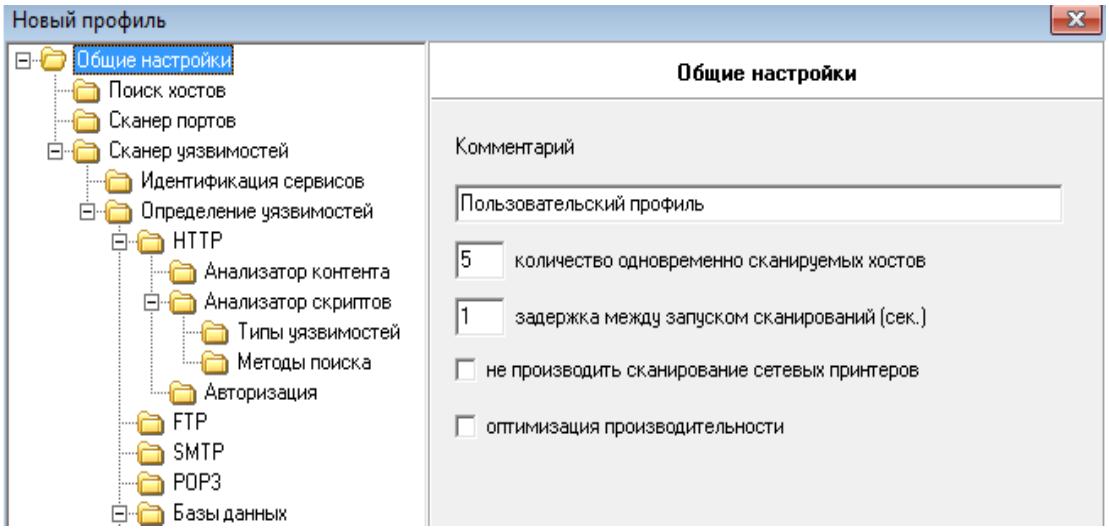


Рисунок 13. Создание нового профиля проверки

Чтобы начать сканирование, необходимо нажать на IP-адрес, далее на сканирование и старт. В окне программы справа появится информация о сканируемом IP-адресе. В окне программы слева будет отображаться информация об удаленном АРМ и результат сканируемого хоста (рисунок 14).

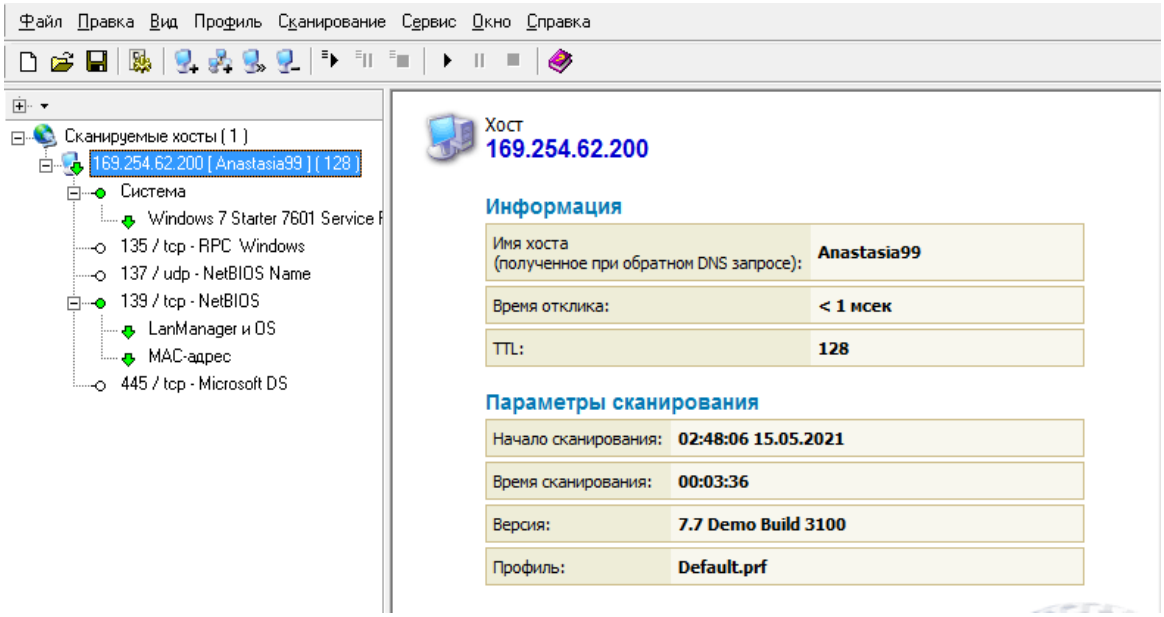


Рисунок 14. Результат сканируемого хоста

В результате сканирования могут быть обнаружены уязвимости, которые выделились бы в окне слева красным или желтым цветом. В данном случае их не было обнаружено. Отсюда можно узнать версию ОС - Windows 7 Starter 7601 Service Pack 1, информацию об имени сервиса - Network Basic Input/Output System, MAC-адрес хоста: 08-00-27-DE-CA-B2, имя сервиса: Microsoft Directory Service, LanManager: Windows 7 Starter 6.1.

Если бы случилось так, что были обнаружены уязвимости, то в отчете были бы даны ссылки, описывающие все угрозы и уязвимости с их последующими устранениями. Одной из основных функций сканера является то, что он может обнаружить максимальное количество в сети «дыр» задолго до того, каких увидит хакер. Сканер может работать удаленно и при этом не потребуется дополнительная установка ПО. Далее для осуществления сканирования можно воспользоваться программой ScanOVAL [7]. ScanOVAL используется для автоматического обнаружения уязвимостей ПО на рабочих станциях под управлением Microsoft Windows.

Программа ScanOVAL выполняет следующие функции:

– загружает XML-файлы с OVAL-описаниями уязвимостей, которые выполнены в соответствии со стандартом «The OVAL Language Specification»;

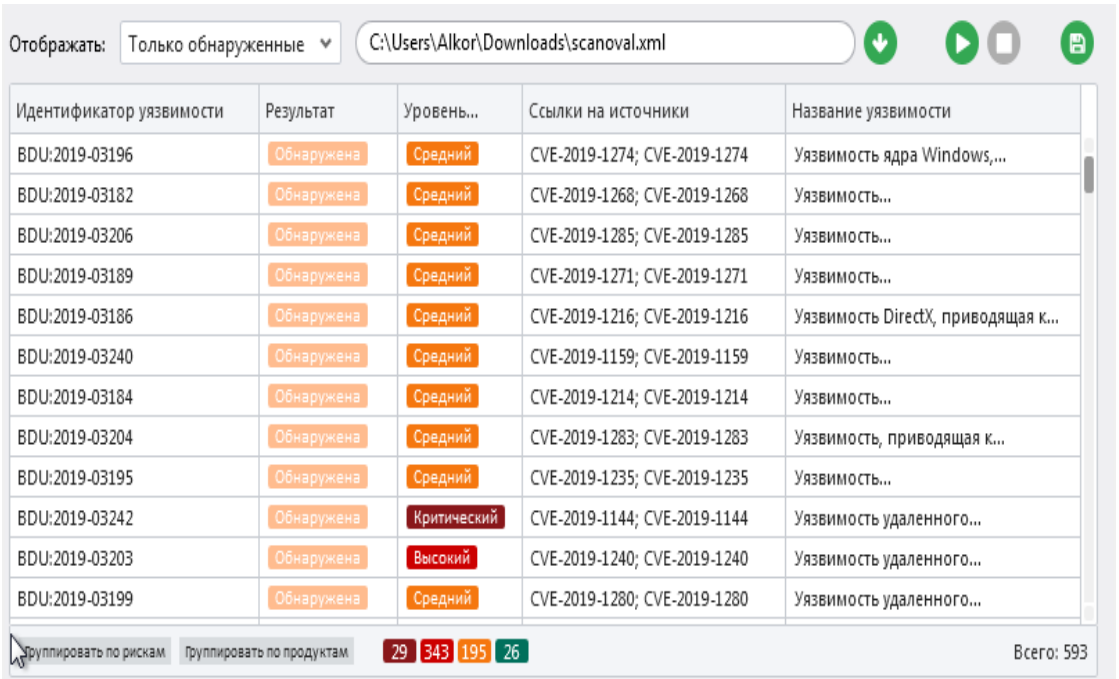
– обнаруживает уязвимости ПО, которое установлено на локальном компьютере под управлением ОС семейства Microsoft Windows.

Программу ScanOVAL необходимо установить на удаленное АРМ с помощью программы UltraVNC. UltraVNC - это такая программа, которая позволяет использовать удаленный компьютер. Будет возможность видеть полный экран удаленного АРМ, двигать мышью, нажимать на клавиши в режиме реального времени. На рабочем месте аудитора должно быть установлено UltraVNC Viewer, с помощью этой программы аудитор будет подключаться к удаленному компьютеру, а на удаленном АРМ – UltraVNC Server. Зная IP-адрес и пароль от сервера, можно подключиться удаленно и установить программу ScanOVAL. Итак, необходимо скачать и установить ПО ScanOVAL и тестовую базу OVAL-описаний. Далее запустить программу ScanOVAL. Следующим шагом для проведения сканирования нужно загрузить XML-файл с OVAL-описаниями. Каждая уязвимость имеет идентификатор, название и уровень угрозы (рисунок 15).

Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники	Название уязвимости
BDU:2021-02431; BDU:2021-0231		Средний	CVE-2021-2284; cpuapr2021	Уязвимость в Oracle VM VirtualBox до 6.1.20 (cpuapr2
BDU:2021-02441; BDU:2021-0231		Низкий	CVE-2021-2297; cpuapr2021	Уязвимость в Oracle VM VirtualBox до 6.1.20 (cpuapr2
BDU:2021-02287		Средний	CVE-2021-29950; mfsa2021-17	Уязвимость в Thunderbird о версии 78.8.1 (mfsa2021
BDU:2021-02475		Средний	CVE-2021-2179; cpuapr2021	Уязвимость в MySQL Server до 5.7.33 и до 8.0.23 (cpu
BDU:2021-02479		Средний	CVE-2021-2230; cpuapr2021	Уязвимость в MySQL Server до 8.0.23 (cpuapr2021)
BDU:2021-02458		Средний	CVE-2021-2193; cpuapr2021	Уязвимость в MySQL Server до 8.0.23 (cpuapr2021)
BDU:2021-02472		Средний	CVE-2021-2202; cpuapr2021	Уязвимость в MySQL Server до 5.7.32 и до 8.0.22 (cpu
BDU:2021-02443		Высокий	CVE-2020-8203; lodash-rails; SNYK	Уязвимость Prototype Pollution в Ruby gem lodash-ra
BDU:2021-02462		Средний	CVE-2021-2164; cpuapr2021	Уязвимость в MySQL Server до 8.0.23 (cpuapr2021)
BDU:2021-02430; BDU:2021-0232		Средний	CVE-2021-2281; cpuapr2021	Уязвимость в Oracle VM VirtualBox до 6.1.20 (cpuapr2
BDU:2021-02456		Средний	CVE-2021-2213; cpuapr2021	Уязвимость в MySQL Server до 8.0.22 (cpuapr2021)
BDU:2021-02466		Средний	CVE-2021-2196; cpuapr2021	Уязвимость в MySQL Server до 8.0.23 (cpuapr2021)
BDU:2021-02265		Высокий	CVE-2021-28471; CVE-2021-28471	Уязвимость удаленного выполнения кода в расшир
BDU:2021-02438; BDU:2021-0231		Средний	CVE-2021-2287; cpuapr2021	Уязвимость в Oracle VM VirtualBox до 6.1.20 (cpuapr2
BDU:2021-02450		Средний	CVE-2021-2310; cpuapr2021	Уязвимость в Oracle VM VirtualBox до 6.1.20 (cpuapr2

Рисунок 15. База уязвимостей ScanOVAL

Далее нужно запустить процесс сканирования на уязвимости (рисунок 16).



Идентификатор уязвимости	Результат	Уровень...	Ссылки на источники	Название уязвимости
BDU:2019-03196	Обнаружена	Средний	CVE-2019-1274; CVE-2019-1274	Уязвимость ядра Windows,...
BDU:2019-03182	Обнаружена	Средний	CVE-2019-1268; CVE-2019-1268	Уязвимость...
BDU:2019-03206	Обнаружена	Средний	CVE-2019-1285; CVE-2019-1285	Уязвимость...
BDU:2019-03189	Обнаружена	Средний	CVE-2019-1271; CVE-2019-1271	Уязвимость...
BDU:2019-03186	Обнаружена	Средний	CVE-2019-1216; CVE-2019-1216	Уязвимость DirectX, приводящая к...
BDU:2019-03240	Обнаружена	Средний	CVE-2019-1159; CVE-2019-1159	Уязвимость...
BDU:2019-03184	Обнаружена	Средний	CVE-2019-1214; CVE-2019-1214	Уязвимость...
BDU:2019-03204	Обнаружена	Средний	CVE-2019-1283; CVE-2019-1283	Уязвимость, приводящая к...
BDU:2019-03195	Обнаружена	Средний	CVE-2019-1235; CVE-2019-1235	Уязвимость...
BDU:2019-03242	Обнаружена	Критический	CVE-2019-1144; CVE-2019-1144	Уязвимость удаленного...
BDU:2019-03203	Обнаружена	Высокий	CVE-2019-1240; CVE-2019-1240	Уязвимость удаленного...
BDU:2019-03199	Обнаружена	Средний	CVE-2019-1280; CVE-2019-1280	Уязвимость удаленного...

Рисунок 16. Найденные уязвимости в ОС Windows 7 с помощью ScanOVAL.

ScanOVAL нашел большое количество уязвимостей в ОС, что является превосходным результатом для сканера уязвимостей. В итоге применение инструментов для проведения аудита отображено в таблице ниже.

Таблица 1

Применение инструментов для проведения аудита

Инструмент	**Условие**	**Элементы**	**Результат**
Nmap	в рамках локальной инфраструктуры организации	список портов, версии ОС, версии программ, уязвимости	полное сканирование удаленного АРМ
XSpider	в рамках локальной инфраструктуры организации	подбор профиля, сетевые узлы, проверка портов, определение доступности	сканирование удаленного АРМ на наличие уязвимостей
VNC (режим 1)	при наличии защищенного трафика	доступ к удаленному АРМ	перехват в управлении удаленного АРМ
VNC (режим 2)	при отсутствии защищенного трафика	доступ к удаленному АРМ	перехват в управлении удаленного АРМ
ScanOVAL	при наличии или отсутствии защищенного трафика	уязвимости	сканирование удаленного АРМ на наличие уязвимостей
IVRE	при наличии или отсутствии защищенного трафика	список портов, версии ОС, сетевые узлы, версии программ, определение доступности	углубленное сканирование удаленного АРМ

С использованием командной оболочки PowerShell существуют разные способы и шаблонные варианты скриптов. Был выбран один из шаблонов, и в него внесены изменения, преобразовав этот скрипт в соответствии с задачами и условиями его эксплуатации. Скрипт позволит получить список всех пользователей, совершавших вход на сервер. Возможность осуществления входа в систему выполняется с использованием конкретного типа входа, основывающийся на значениях EventID и EntryType, было вы-

брано значение EventID = 528 (осуществление успешного входа на компьютер), EntryType = 10 (успешное выполнение удаленного входа пользователя на компьютер). Команда будет выглядеть следующим образом:

Get-EventLog security -message "*Тип входа:?10*" -after (Get-date -hour 0 -minute 0 -second 0) | ?{$_.eventid -eq 528

В результате будет выведен список со временем успешного входа. Можно изменить команду так, чтобы в таблице выводились три параметра: время, имя пользователя, IP адрес. Далее необходимо создать объект и необходимо включить в него все необходимые сведения. Скрипт, который позволит вывести нужную информацию указан в Приложении 1.

В результате при запуске этого скрипта будет отображено имя пользователя, время и IP-адрес (рисунок 17). Также можно путем изменения параметров значений EntryType и EventID можно настроить скрипт на выполнение той задачи, которая потребуется.

Рисунок 17. Результаты использования скрипта

Если сравнивать применяемые инструменты по отдельности, то в конечном результате не удастся получить полный перечень информации, необходимый для проведения аудита. Например, использование одной программы Nmap не позволит получить информацию об уязвимостях удаленной инфраструктуры организации. Также и программа XSpider не сможет осуществить сканирование системы за пределами ДМЗ. Программа ScanOVAL может осуществлять сканирование локально, поэтому было принято решение воспользоваться программой UltraVNC для его установки на удаленном АРМ. Поэтому приоритетнее всего будет использование комплекса различных программ, с помощью которых получится собрать необходимую информацию для более качественной оценки об удаленной организации.

2.Практическая часть

2.1Нужно определить:

- Ограничения сетевой трансляции;

- Тип доступа к компонентам ИС;
- Стабильность сетевой среды.

2.2 В соответствии с выбранной моделью аудита необходимо:

Применить порядок действий для сбора информации об удаленной организации:

– иерархическая структура организации;

– информация об уровне конфиденциальности данных, которые хранятся, обрабатываются и передаются по каналам связи с использованием компьютерных технологий;

– руководящие документы по хранению, обработке и передаче информации;

– положения о защите информации;

– список информации, составляющей коммерческую или служебную тайну в организации.

2.3 Получить с помощью инструментария (в соответствии с выбранной моделью) информацию об имеющихся средствах вычислительной техники:(

– количество серверов;

– тип ОС, версия ОС (patch, service pack);

– сетевые протоколы;

– дополнительная документация;

– перечень используемых средств защиты информации.

2.4 Исследовать с применением инструментария (в соответствии с выбранной моделью) информацию о топологии сети:

– распределение серверов по сегментам;

– информация о распределении рабочих станций;

– осуществление выхода в Internet;

– типы оборудования сети, их версии;

– информация о применении системного сетевого ПО;

2.5 Собрать информацию о клиентских рабочих местах:

– место установки, количество и тип;

– описание применения аппаратных платформ, аппаратное обеспечение;

– перечень используемых средств защиты информации.

На основе выбранной модели аудита необходимо осуществить следующие действия:

2.6 Для модели аудита (в рамках локальной инфраструктуры организации):

2.6.1 Организовать встречу с использованием средств видеосвязи для заполнения необходимых анкет, беседы с персоналом;

2.6.2 Предоставить IP-адрес удаленного АРМ для его полного или частичного перехвата в управлении;

2.6.3 Запустить программу сканирования сетевых интерфейсов для полного сканирования, удаленного АРМ (список портов, версии ОС, версии программ, определение доступности, уязвимости);

2.6.4 Запустить сканер уязвимостей для сканирования системы на наличие уязвимостей с возможностью индивидуального подбора профиля в заданных условиях для данной модели;

2.6.5 Запустить инструмент сетевой разведки для углубленного сканирования системы (список портов, версии ОС, версии программ, определение доступности, сетевые узлы и другое);

2.6.6 Составить отчет по результатам сканирования и проверок.

2.7 Для второй модели аудита (с использованием защищенного трафика):

2.7.1 Организовать встречу с использованием средств видеосвязи;

2.7.2 Предоставить IP-адрес удаленного АРМ для его полного или частичного перехвата в управлении;

2.7.3 Запустить программу сканирования сетевых интерфейсов для полного сканирования, удаленного АРМ (список портов, версии ОС, версии программ, определение доступности, уязвимости);

2.7.4 Запустить инструмент сетевой разведки для углубленного сканирования системы (список портов, версии ОС, версии программ, определение доступности, сетевые узлы и другое);

2.7.5 Установить программу удаленного доступа, которая послужит средством получения локального доступа в исполняемую среду ОС;

2.7.6 Правильно настроить программу удаленного доступа и выбрать режим с использованием защищенного трафика;

2.7.7 Установить сканер для автоматического обнаружения уязвимостей.

Контрольные вопросы:

1. Рассмотрите особенности описания уязвимостей информации, защищенности информации, угроз безопасности информации, защите информации, которые используются при сканировании. Перечислите источники угроз безопасности информации.
2. Охарактеризуйте основные принципы функционирования программ поиска уязвимостей и собора данных.
3. Проясните положительные и отрицательные особенности программ поиска уязвимостей и собора данных.

Практическая работа № 3. Факторы оценки риска

Программно-аппаратные средства: стандартные средства Microsoft Office.

1.Теоретический материал

В простейшем случае для оценки рисков учитываются два фактора: вероятность происшествия и тяжесть возможных последствий. Считается, что риск тем больше, чем выше вероятность происшествия и больше тяжесть последствий. Сказанное можно выразить формулой:

$$R = P * C, \quad (1)$$

где R – риск, P – вероятность происшествия, C – цена потерь.

Если переменные P и C являются количественными величинами, то риск– это оценка математического ожидания потерь.

Если же переменные P и C являются качественными величинами, то операция умножения не определена, и формула 10.1 в явном виде применяться не может. Однако именно использование качественных величин – наиболее часто встречающаяся ситуация. Рассмотрим данный случай подробнее.

Сначала должны быть определены значения лингвистической переменной вероятности события, например, по такой шкале:

- A – вероятность события стремиться к нулю в рассматриваемый период времени;
- B – событие редкое в рассматриваемый период времени;
- C – вероятность события в рассматриваемый период времени составляет примерно 0,5;
- D – скорее всего событие произойдет в рассматриваемый период времени;
- E – событие произойдет в рассматриваемый период времени с вероятностью 0,9.

Так же определяется значение второй лингвистической переменной – серьезности происшествия:

- H – воздействие не важно для состояния ИБ;
- HC – незначительное происшествие: последствия легко устранимы, затраты на ликвидацию последствий невелики, воздействие на информационную технологию незначительно;
- Ср – происшествие средней важности (ликвидация последствий не связана с крупными затратами воздействие на информационную технологию невелико и не затрагивает критически важные задачи);
- B – важное для системы событие (происшествие с серьезными последствиями: ликвидация последствий связана с серьезными затратами, воздействие на информационные технологии ощутимо и затрагивает выполнение критически важных задач);

- К – критическое для системы событие (происшествие приводит к невозможности решения критически важных задач).

Для оценки рисков можно применять любую шкалу, градации в которой можно определять как лингвистические переменные. Обычно рассматривают три лингвистические переменные: низкий риск, средний риск, высокий риск, как показано в таблице. Шкалы факторов риска и сама таблица могут быть определены иначе и иметь другое число градаций (таблица 2).

Таблица 2

Табличная двухфакторная оценка риска

Ресурс\уровень риска	N	НС	Ср	В	К
A	Низкий риск	Низкий риск	Низкий риск	Средний риск	Средний риск
B	Низкий риск	Низкий риск	Средний риск	Средний риск	Высокий риск
C	Низкий риск	Средний риск	Средний риск	Средний риск	Высокий риск
D	Средний риск	Средний риск	Средний риск	Средний риск	Высокий риск
E	Средний риск	Высокий риск	Высокий риск	Высокий риск	Высокий риск

При применении подобных методик оценки рисков необходимо учитывать следующие особенности:

- значения шкал должны быть обоснованы, и восприниматься однозначно и одинаково всеми участниками аудита;
- требуются обоснования выбранной таблицы рисков.

Подобные методики широко применяются при проведении анализа рисков базового уровня.

В большинстве методик, рассчитанных на более высокие требования, чем базовый уровень, используется оценка рисков по трем факторам: угроза, уязвимость, цена потери.

Эти факторы определяются следующим образом:

1. Угроза – совокупность условий и факторов, которые могут стать причиной нарушения целостности, доступности или конфиденциальности информации.

2. Уязвимость – слабость в системе защиты, которая делает возможным реализацию угрозы.

3. Стоимость потери – это качественная или количественная оценка степени серьезности происшествия.

Вероятность происшествия, которая в данном подходе может быть объективной или субъективной величиной, зависит от уровней (вероятностей) угроз и уязвимостей:

$$P_{происшест} = P_{угрозы} * P_{уязвимости} \quad (2)$$

Соответственно риск определяется следующим образом:

$$R = P_{угр} * P_{уязв} * C \ . \quad (3)$$

Выражение 2 можно рассматривать как математическую формулу, только если используются количественные шкалы. Эту шкалу можно преобразовать в качественную. В этом случае применяются различного рода таблицы для определения риска в зависимости от трех факторов.

Величина риска может оцениваться в шкале от 0 до 8, или иным образом (специалист по ИБ самостоятельно может разработать требуемую шкалу в зависимости от условий и требований), со следующими определениями уровней риска (таблица 3):

1 – риск практически отсутствует;

2 – риск очень мал и т. д.

Таблица 3

Трехфакторная оценка риска

Степень серьезности происшествия (цена потери)	Уровень угрозы								
	Низкий			Средний			Высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
Незначительная	0	1	2	1	2	3	2	3	4
Несущественная	1	2	3	2	3	4	3	4	5
Умеренная	2	3	4	3	4	5	4	5	6
Серьезная	3	4	5	4	5	6	5	6	7
Критическая	4	5	6	5	6	7	6	7	8

В данной таблице приведены уровни уязвимости (Н, С, В, означают соответственно низкий, средний высокий).

Практические сложности в реализации этого подхода следующие:

- должен быть собран весьма обширный материал о происшествиях в данной области;

- применение этого подхода оправдано далеко не всегда. Если информационная система достаточно крупная (содержит много элементов, расположена на обширной территории), имеет давнюю историю, то подобный подход, скорее всего, применим. Если же система сравнительно невелика, использует новейшие элементы технологии (для которых пока нет достоверной статистики), то оценки угроз могут оказаться недостоверными.

В настоящее время известно множество табличных методов оценки рисков ИБ организации. Важно, чтобы организации сама выбрала для себя подходящий метод, который обеспечивал бы корректные и достоверные воспроизводимые результаты.

Трёхфакторную оценку риску можно рассмотреть более подробно. Ее можно интерпретировать следующим образом:

$$R = P_a * P_y * C * K, \quad (4)$$

где *Pa* - вероятность проявления угрозы (*Pa*= (число активных негативных воздействий) \ (общее число обращений к компоненту)), *Py* - вероятность успешной эксплуатации уязвимостей, *C* – стоимость компонента, *K* – коэффициент актуальности ресурса.

Как видно параметры вероятности угроз и проявления уязвимостей можно конкретизировать и, таким образом, формула классического типа, становится многофакторной. Количество учитываемых факторов зависит от меры детализации рассмотрения риска. Допусти в организации определены следующие примерные угрозы:

1. Неправомерные действия нал внутренними документами компании, не затрагивающие конфи информацию
2. Раскрытие конфи документов компании
3. Изменение или удаление информации из базы данных об отправлениях
4. Заражение комп вирусами
5. Несанкционированный доступ к системе третьими лицами
6. Преднамеренное изменение параметров настроек средств защиты (антивирусов)
7. Сбой системы или отказ в работе
8. Кража оборудования.

Следуя формуле многофакторной оценки риска, результаты анализа их будет следующими**:**

Таблица 4

Результаты многофакторной оценки риска

№	Pa	Py	C	K	R
1	0,27	1,971	2 000	0,6	638,604
2	0,14	0,728	7 500	0,8	611,52
3	0,1	0,235	500	0,4	4,7
4	0,04	0,36	5 000	0,8	57,6
5	0,042	0,2856	5 000	0,8	47,9808
6	0,04	0,288	5 000	0,8	46,08
7	0,08	0,208	500	0,2	1,664
8	0,02	0,134	15 000	0,6	24,12
Суммарный риск					179,0336

2.Практическая часть

2.1 Изучить основной теоретический материал.

2.2 Для выбранной организации с учетом результатов инвентаризационных этапов аудита инфраструктуры организации реализовать следующее:

- разработать шкалу лингвистических переменных;
- произвести ранжирование угроз ИБ вашей ИС;
- на примере, указанном в теоретическом материале, проанализировать угрозы и риски, создать таблицы с результатами анализа для двухфакторной оценки риска;
- на примере, указанном в теоретическом материале, проанализировать угрозы и риски, создать таблицы с результатами анализа для трехфакторной оценки риска.

2.3 Произвести анализ рисков в выбранной организации по многофактной оценки риска (3) по примеру в параграфе.

2.4 Создать отчет с указанием проведенных исследований

Контрольные вопросы

1. Дайте определения безопасности информации, уязвимости информации, защищенности информации, угрозам безопасности информации, защите информации.
2. Охарактеризуйте основные принципы системной классификации угроз безопасности информации.
3. Поясните суть рассматриваемой методики оценки уязвимости информации.

Практическая работа № 4. Оценка риска с использованием координатной плоскости

Программно-аппаратные средства: стандартные средства Microsoft Office.

1.Теоретический материал

При первоначальных этапах обработки информации, собранной по итогам инвентаризации, при уже известных уязвимостях, примерной оценке стоимости потерь (относительно рассматриваемых компонентов) информационной системы можно (для корректирования будущих шагов при анализе рисков) предварительно наметить направление рассмотрения угроз, на которые следует сосредоточить позже своё внимание.

Соответственно, первоначально следует рассматривать риски примерно, используя различные графические способы. При этом уровень опасности угроз, которые, конечно, предполагают и рассмотрение уязвимости, можно оценивать, используя лингвистические переменные.

Очевидно, при начале анализа вероятность негативного события невозможно оценить сколько-нибудь точно. Для этого нет ни теоретических предпосылок, ни накопленного статистического базиса. Нет возможности и для обоснованной оценки влияния контрмер на вероятности. Наконец негативные события могут не быть независимыми. Одно из них может исключать другое (например, пожар и затопление) или, напротив, вызывать каскадный эффект, как это бывает при перегрузке критически важных компонентов. В силу приведенных здесь соображений целесообразно трактовать риски не как числовые значения, а как точки на плоскости, где координатными осями служат вероятности и потери (Рисунок 18).

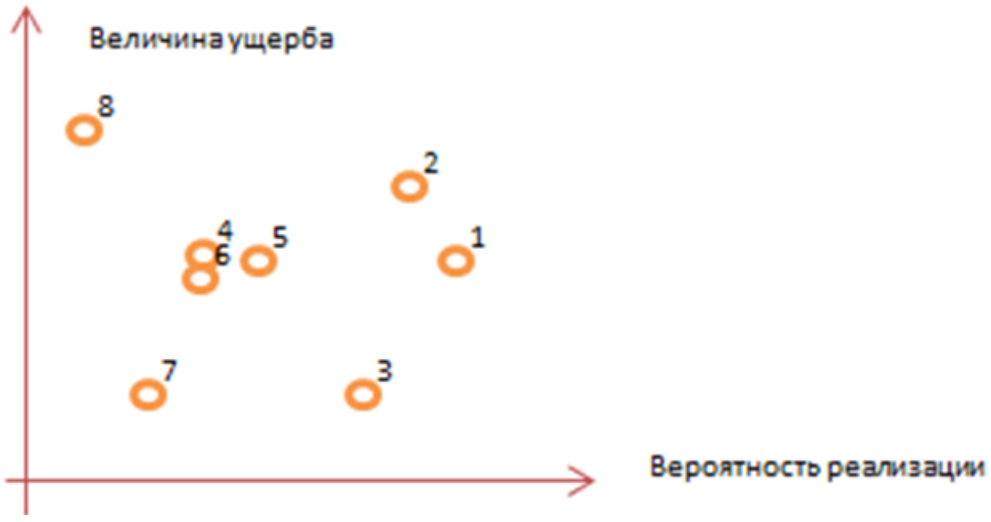


Рисунок 18. Представление рисков в виде точек на координатной плоскости

Для начального этапа анализа риски можно проанализировать, используя координатные плоскости. Для этого требуется формулу риска (1) представить в виде координатных плоскостей. Соответственно, для двухфакторной оценки риска ось абсцисс будет являться мерой угрозы некоторого события, фактора, а ось ординат – мерой ущерба рассматриваемых событий. Требуется разместить на координатной плоскости точки событий или факторов в соответствии с параметрами угроз и потерь (ущерба), отложенными по осям координатной плоскости.

Подобное графическое отображение позволяет наглядно продемонстрировать уровень риска компрометации информации в организации. Обратите внимание на то, что некоторые виды рисков будут группироваться в определённой области координатной плоскости. Это может указывать на существование некого критически важного фактора, влияющего на проявление угроз и уязвимостей. На основании сделанных выводах о сосредоточии вершин рисков, можно прогнозировать наиболее эффективные меры предотвращения реализации рисков. Очевидно, подобный анализ носит приблизительный характер. Однако результаты подобного анализа позволят изначально ориентироваться в исследовании результатов на определённый спектр задач, связанных исследованием и поиском средств нивелирования угроз, что позволит минимизировать время анализа. Такую координатную плоскость, но в трехмерном виде, можно построить, используя формулу трехфакторной оценки риска (2).

2.Практическая часть

2.1 Формулу риска (1) представить в виде координатных плоскостей (ось абсцисс будет являться мерой угрозы н0 фактора, а ось ординат – мерой ущерба).

2.2 Ориентируясь на результаты аудита выбранной организации, разместите на координатной плоскости точки событий в соответствии с параметрами угроз и потерь (ущерба).

2.3 Определите группы рисков в определённой области координатной плоскости. Сделайте предположение наиболее важных критических факторах, влияющих на проявление угроз и уязвимостей.

2.4 На основании сделанных выводах о сосредоточии вершин рисков предложите эффективные меры предотвращения реализации рисков.

2.5 Такую координатную плоскость, но в трехмерном виде, можно построить, используя формулу трехфакторной оценки риска (2).

2.6 Результаты занести в отчет.

Контрольные вопросы:

1. Дайте определения уязвимости информации, защищенности информации, угрозам безопасности информации, защите информации рассматриваемой методике

2. Охарактеризуйте основные принципы построение **оценки риска на координатной плоскости**.

3. Проясните положительные и отрицательные особенности методики оценки уязвимости информации.

Практическая работа № 5. Дерево угроз и уязвимостей

Программно-аппаратные средства: стандартные средства Microsoft Office.

1.Теоретический материал

Представление рисков в виде точек на плоскости является удачным с психологической точки зрения, поскольку оно разделяет два разных аспекта риска — вероятность и воздействие и наглядно показывает, с чем в первую очередь нужно бороться и насколько это удалось (Рисунок 19).

Можно воспользоваться еще одним представлением рисков — в виде деревьев уязвимостей, угроз и контрмер. Здесь Vi — уязвимости, Ti,j — угрозы, эксплуатирующие уязвимости, Ci,j — контрмера, нейтрализующая угрозу (i,j), Li,j — недостаток контрмер для угрозы (i,j) [13].

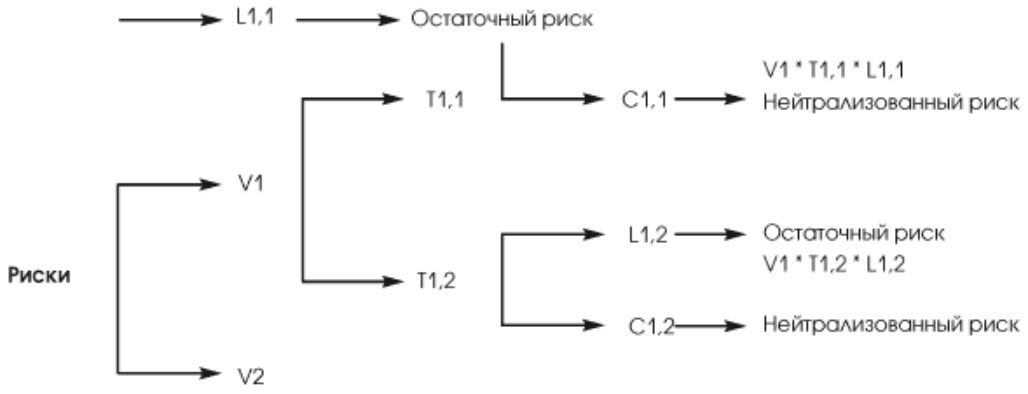


Рисунок 19. Представление рисков в виде дерева уязвимостей, угроз и контрмер.

Значение для Vi, Ti,j, Li,j и Ci,j целесообразно нормировать, так чтобы суммы по i Vi и Ti,j равнялись 1, а также сумма Li,j , Ci,j должна равняться 1.

Кроме вероятностных параметров, в оценке рисков участвуют константы — критичность активов (CA) и их стоимость (CC) (Рисунок 20). Общая ожидаемая сумма потерь равна произведению общего остаточного риска на величины CA и CC [13].

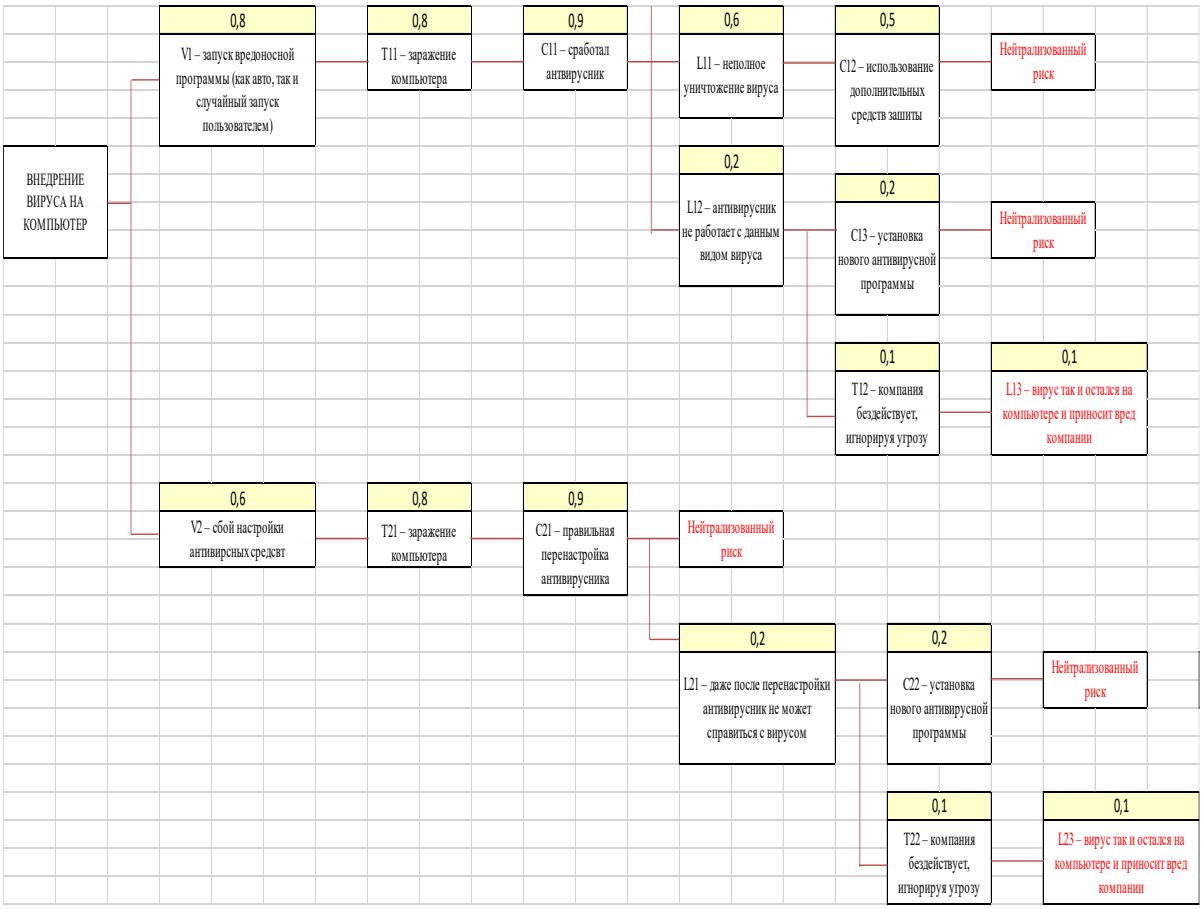


Рисунок 20. Граф компрометации

2.Практическая часть

1. Изучить основной теоретический материал о **дереве уязвимостей, угроз и контрмер**. Изучите материал в Приложении № 1.

2. Произведите анализ угроз ИБ ИС выбранной организации, определите их класс.

3. По изученной методике **постройте дерево угроз и уязвимостей** относительно выбранной организации, определив основные параметры безопасности, требуемые для реализации методики.

4. Определите угрозы, представленные на Рисунок 21 графа угроз ИБ данной ИС. Укажите, как представленное дерево может быть интегрировано в вашу аналитическую модель?

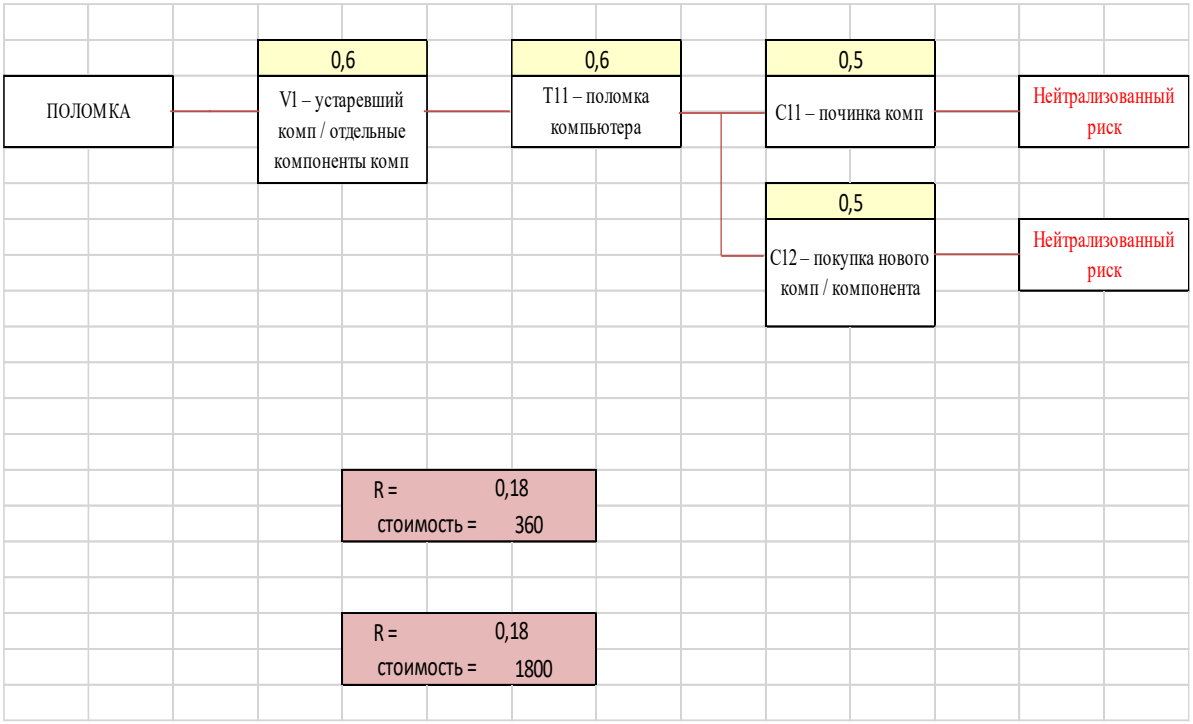


Рисунок 21. Граф компрометации

5. Сделайте выводы по результатам анализа вашей ИС.
6. Определите угрозы, представленные в приложении 1.
7. Результаты исследования внесите в отчет.

Контрольные вопросы:

1. Укажите особенности определения уязвимости информации, защищенности информации, угроз безопасности информации, защите информации в рассматриваемой методике.
2. Охарактеризуйте основные принципы построения **дерева угроз и уязвимостей**.
3. Проясните положительные и отрицательные особенности данной методики оценки уязвимости информации.

Практическая работа № 6. Оценка риска с использованием пороговых значений

Программно-аппаратные средства: стандартные средства Microsoft Office.

1.Теоретический материал

Можно предложить и другие формализмы для управления рисками. Предположим, имеется M пар (актив, угроза). Для каждой такой пары риск вычисляется по обычной формуле (4):

$$R_k = P_i * I_j \ . \qquad (4)$$

Здесь k — номер пары, P_i — вероятность реализации угрозы по отношению к "парному" активу, I_j — воздействие реализации этой угрозы на актив, R_k — величина риска.

Пусть, далее, риски считаются допустимыми, если для всех пар (k) величина $R_k <= R_a$, где R_a — порог допустимости. Избыточные риски, которые требуется нейтрализовать, можно выразить соотношениями вида (5):

$$r_k = R_k - R_a, \textit{если } R_k > R_a,$$
$$r_k = 0, \textit{если } R_k \le R_a \qquad (5)$$

Пусть N — число положительных пар рисков (rk), т. е. число пар (актив, угроза), риски которых нуждаются в нейтрализации. Отбросим нулевые избыточные риски и перенумеруем оставшиеся. Можно вычислить среднее значение избыточного риска ($rMean$), воспользовавшись формулой (6) [13]:

$$r_{Mean} = ((\textit{сумма по } k \textit{ от } 1 \textit{ до } N)\ r_k) \div N \ . \qquad (6)$$

Значение $rMean$ можно рассматривать не только как средний избыточный риск, но и как оценку безопасности информационной системы в целом. Эту оценку можно нормализовать, воспользовавшись формулой [13]:

$$r_{Mean}\ N_{rorm} = r_{Mean} \div (R_{\max} - R_a) \ , \qquad (7)$$

где R_{max} — максимальный из возможных рисков R_k, т. е. произведение максимального из возможных значений P_i и I_j в выбранной шкале измерений.

Значения $rMeanNorm$, близкие к 0, характеризуют уровень информационной безопасности ИС как весьма высокий. Близкие к 1 значения характерны для слабо защищенных информационных систем. При желании отрезок [0, 1] можно разбить на интервалы, выделив тем самым нужное число уровней безопасности [13].

Кроме среднего арифметического, можно вычислить среднее квадратичное значение положительных избыточных рисков (σ) по формуле ниже (8):

$$\sigma = \sqrt{(((\sum_{1}^{n} k) r_k * r_k)) \div N)} \, . \qquad (8)$$

Как и средний избыточный риск, среднее квадратичное значение можно нормализовать:

$$\sigma_{Norm} = \sigma \div (R_{\max} - R_a) \ . \qquad (9)$$

Нормализованное среднее квадратичное значение, как и величину *rMeanNorm*, можно напрямую использовать для оценки уровня информационной безопасности организации, если разбить отрезок [0, 1] на соответствующее число интервалов. Значения, близкие к 0, свидетельствуют о высоком уровне защищенности, близкие к 1 — о низком. Преимущество среднего квадратичного значения по сравнению со средним арифметическим в том, что первое более устойчиво к добавлению пар с небольшими избыточными рисками и более чувствительно к аномально высоким рискам.

2. Практическая часть

2.1 Изучить основной теоретический материал о **оценке риска с использованием пороговых значений**.

2.2 Произвести анализ угроз ИБ ИС выбранной организации, определить их класс.

2.3 Составить и внести в отчет перечни типов угроз ИБ и информационные ресурсы, присутствующие в данной ИС.

2.4 Определить пороговые значения риска для выбранной системы, структуры.

2.5 По изученной методике оценить риски ИБ данной ИС, определить величину избыточных рисков

2.5 Сделайте выводы по результатам анализа вашей ИС. Результаты исследования внесите в отчет.

Контрольные вопросы:

1. Укажите особенности определения уязвимости информации, защищенности информации, угрозам безопасности информации, защите информации в рассматриваемой методике.

2. Охарактеризуйте основные принципы методики **пороговых значений риска.**

3. Проясните положительные и отрицательные особенности данной методики оценки уязвимости информации.

Практическая работа № 7. Расчет графа компрометации

Программно-аппаратные средства: стандартные средства Microsoft Office.

1.Теоретический материал

Инициирование современной сетевой атаки, процесс ее развертывания, как правило, контролируются злоумышленником (хакером). Его уровень квалификации (статус), определяемый в процессе отслеживания атаки, возможно использовать не только для выявления степени опасности угрозы, но и для прогнозирования действий атакующего.

Профессиональный хакер, в отличие от непрофессионала, имеет четко определенные цели: кража информации, прослушивание трафика. Стараясь получить наибольшее количество информации за один сеанс работы, он будет стремиться как можно дольше находиться в системе в режиме скрытого доступа. Наиболее эффективным способом выявления подобного злоумышленника является сбор аномалий в системе и контроль операций над критически важными данными. Соответственно, целесообразно в список параметров определения пути атаки добавить и параметр контроля состояния доступа к критически важной информации с учетом времени доступа. Эти особенности поведения можно использовать и при эвристическом анализе угроз безопасности, и для создания модели нарушителя.

Для осуществления несанкционированного доступа к данным (цели атаки) злоумышленнику потребуется осуществить несколько этапов вторжения. Это означает введение промежуточных целей в трассу (граф) атаки в соответствии с каждым этапом. При этом ответвления ко всякой промежуточной вершине (подцели) будут регламентированы необходимостью решения основной целевой задачи и присутствием промежуточных барьеров, параметры стойкости которых зависят, в том числе, от меры квалифицированности злоумышленника. Соответственно, параметр стойкости важно учесть и при прогнозировании развертывания атаки.

Трасса атаки непрофессионального злоумышленника будет отличаться множеством направлений и путей, которые в ситуации непреодоления барьера будут замыкаться на исходной точке атаки или на промежуточных точках перед барьерами. При этом переходы на промежуточные узлы в силу неизвестности целей злоумышленника определить будет трудно. Выявить их возможно с помощью логических операций (И, ИЛИ), условия которых будут содержать соответствующие параметры стойкости барьеров. По интенсивности использования переходов с заданными параметрами можно судить о квалификации атакующего, что даст возможность определить направление и ход развертывания атаки в целом.

Фактически вопрос определения квалифицированности связан с проблематикой построения модели нарушителя и, в дальнейшем, использования таковой для расчетов параметров атаки формальными методами. Для определения актуальности атак и построения модели злоумышленника необходимо произвести детальное категорирование нарушителей по уровню знаний и возможностей.

Первая категория нарушителей, классифицируемых по уровню знаний, предполагает наличие понимания у злоумышленника принципов построения и работы вычислительных систем, сетевых протоколов, использование стандартного набора программ. Вторая категория подразумевает осведомленность нарушителя в области сетевых технологий, а также наличие опыта работы со специализированными программными продуктами и утилитами, понимание работы протоколов, используемых в защищенных компьютерных сетях. Третья категория нарушителей должна обладать знаниями в области программирования. К четвертой категории можно отнести тех, кто имеет достаточно подробную информацию об атакуемом объекте (о его защите, способах обнаружения вредоносной деятельности). Последняя категория нарушителей наиболее опасная поскольку предполагает то, что атакующие являются инсайдерами. Они могли быть разработчиками или принимать участие в реализации системы обеспечения информационной безопасности на стороне провайдера или клиента.

По уровню опасности доступных средств воздействия вводится ряд категорий. Первая категория предполагает применение методов социальной инженерии: манипуляцию, подкуп, шантаж. Вторая категория включает пассивные средства: технические и программные средства перехвата без модификации компонентов системы. Третья категория подразумевает использование только штатных средств или недостатков СЗИ для ее преодоления (несанкционированные действия с использованием разрешенных средств), компактные носители информации, анализаторы трафика (снифферы), сканеры, утилиты. Четвертая категория включает методы и средства активного воздействия: модификация и подключение дополнительных технических устройств, подключение к каналам связи, внедрение программных и аппаратных закладок, эксплойтов, использование специальных инструментов и вредоносных программ.

Таким образом, при разработке модели нарушителя на основе его качественных характеристик требуется учесть: уровень знаний нарушителя, его цели, средства воздействия на атакуемый объект, последовательность этапов атаки. Наиболее часто встречаются злоумышленники со средней или низкой квалификацией, т. е. принадлежат по классификации знаний к первой, второй и третьей категориям. К группе средней квалифицированности можно отнести профессиональных хакеров. Категорию злоумышленников, определяемую типовым набором знаний у нарушителя о методах построения и эксплуатации вычислительных систем, сетевых протоколах, следует соотнести с группой непрофессионалов. Порядок их действий не предполагает последовательного и целенаправленного применения специальных средств доступа к компрометируемым ресурсам. Однако широко используются методы социальной инженерии, совмещенные с методами неконтролируемого заражения компьютера-клиента с помощью технологий спам-рассылки, подкупа, шантажа, визуального сбора информации.

Злоумышленники, обладающие достаточными знаниями в области сетевых технологий (принадлежащие ко второй категории по знаниям), имеющие опыт работы со специализированными программными продуктами и утилитами, протоколами, используют методы и средства активного воздействия (средства воздействия третьей и четвертой категорией). Наиболее часто встречаемые в этом случае атаки следующие: XSS, MITM, спуффинг, фишинг, DoS. Последовательность действий атакующего при осуществлении атак MITM, Спуффинг предполагает следующие фазы: разведка, подключение к сети, прослушивание, выявление сетевых характеристик маршрутизирующих устройств, параметров клиентских терминалов, компрометация ресурса сети (через подмену адреса). При проведении атак XSS, фишинг, DoS известна следующая последовательность: разведка, подключение к виртуальной сети, получение параметров клиентских терминалов, подмена средствами служб виртуального доступа компрометируемого узла. Целями данных атак, как правило, является компрометация системной части служб обмена данным, и поддержки соединений на транспортном и сетевом уровне (для атаки типа спуффинг, MITM), и на прикладном уровне (XSS, фишинг).

Злоумышленники третьей категории, имеющие знания характерные не только для более низких категорий нарушителей, но и обладающие высокой степенью осведомленности в области программирования, системного проектирования и эксплуатационных характеристиках атакуемых объектов, используют штатные средства или недостатки СЗИ для ее преодоления, средства перехвата сетевых данных. Ими могут применяться методы и средства активного воздействия третьей категории. К типам атак, требующим указанных знаний и навыков, относятся: атаки на приложения, MITM на защищенный канал связи (SSL), XSS, SQL-инъекция. Средства и методы воздействия можно отнести по классификации не только к третьей, но и к четвертой категории. Целями злоумышленников являются: компрометация системной части служб обмена данными и поддержки соединений на транспортном и сетевом уровне, компрометация хоста пользователя облачных сервисов и/или получение возможности деструктивных действий на сервере с помощью средств web-сервисов виртуальных систем доступа, компрометация вычислительных ресурсов пользователей виртуальных сервисов.

В случае применения атаки MITM на защищенный канал SSL подразумевается следующая последовательность этапов атаки: разведка, подключение к сети, вторичная разведка, определение топологии исследуемой сети, определение свойств систем маршрутизирующих узлов, подмена сертификата сервера, компрометация ресурса сети. При атаках XSS, SQL-инъекции компрометация системы состоит из этапов: разведка, обход фильтрации переменной, внедрение вредоносного кода, получение параметров клиентских терминалов, компрометация ресурсов сети.

Приведенные категориальные оценки позволяют построить качественную модель нарушителя. Однако их можно использовать и для количественного расчета уязвимости некоторого элемента системы при условии, что каждая оценка будет представлена в величине вероятности, учитывающей рассматриваемые параметры модели нарушителя:

P_k - вероятность соответствия к-й категории (знания) нарушителя в информационной системе требуемой категории для достижения к целевого узла.

P_i - вероятность эксплуатационной пригодности средства воздействия i-й категории;

P_{ki} - вероятность наладки несанкционированного доступа k-й категории нарушителя к целевому компоненту информационной системы с помощью средств воздействия.

P_{pki} - вероятность правильной эксплуатации средства воздействия i-й категории с учетом соответствия k-й категории (знания) нарушителя в информационной системе с требуемым уровнем знаний для достижения к целевого узла.

Тогда в соответствии со следующей формулой возможно получить уровень потенциальной уязвимости защищаемого компонента как некоторого целевого узла:

$$P_y = P_k * P_i * P_{ki} * P_{pki}, \quad (10)$$

где P_y – потенциальная уязвимость компонента системы.

При этом получаемая величина будет соответствовать качественной характеристике, определяемой в категориальной форме, характерной для некоторого множества атак. С другой стороны, ее можно использовать при вычислении временных параметров сетевой атак, посредством приравнивания параметров успешности подпроцессов атаки и параметров уязвимости, полученных на основе категориального анализа нарушителя в известной формуле расчета времени атаки [13]:

$$T = t_1 * P_1 + t_2 * (1 - P_1) * P_2 + t_3 * (1 - P_1) * (1 - P_2), \quad (11)$$

где t_1 — ожидаемое время завершения подпроцесса P_1(*известна, по крайней мере, одна уязвимость, и атакующий располагает средствами ее использования*); t_2 — ожидаемое время завершения подпроцесса P_2 (*известны уязвимости, но атакующий не располагает средствами их использования*; t_3 — ожидаемое время завершения подпроцесса 3 (не *известны уязвимости, но атакующий не располагает средствами их использования*), появление которого зависит от успешности подпроцессов P_1, P_2.

Следуя логике расчетов, необходимо отметить, что успешность взлома некоторого компонента системы зависит от степени квалифицированности злоумышленника, т. е. от его знаний, умений, информированности, целей. Получаемую величину времени компрометации (Т) можно рассматривать как параметр достижения некоторой промежуточной цели в общем графе атаки. Тогда количественный состав множества фиксированных по времени успешных и неуспешных нарушений (определяется по времени обнаружения меньшего, чем время компрометации) будет указывать на количество задействованных целевых элементов, переходов от одного элемента к другому, что, в свою очередь, является показателем квалифицированности нарушителя (профессионал или непрофессионал). Данные показатели целесообразно использовать в продукционных правилах для определения трассы атак и конкретизации параметров компрометации.

Таким образом, статус злоумышленника, при анализе которого учитывается уровень квалифицированности, степень заинтересованности, мотивы поведения, можно использовать и при анализе свойств атаки, и как условный параметр в продукционных правилах прогнозирования сетевых атак, для определения их свойств, стадий, трасс. Мера квалифицированности может быть применена для составления и корректировки модели нарушителя (Рисунок 22).

Рис 22. Граф компрометации (кража документов компании)

Определение показателей времени атаки первоначальной и укрепленной конфигурации системы требует генерации двух графов компрометации. Если в укрепленной системе уязвимостей меньше, а кратчайший путь успешной атаки имеет большую длину для произвольной квалификации злоумышленников, можно переходить к оценке снижения рисков.

На рисунке 23 представлены расчеты для привенного графа компрометации новых интегрированных средств защиты.

без контрмер		
T1 = 28,6	время, ч	вероятность
старт	24	0,3
начало атаки	3	
получение привелегий пользавтеля	0,1	
получение привелегий супер пользавтеля	1	
целевой узел	0,5	
T2 = 29,6	время, ч	вероятность
старт	24	0,4
начало атаки	3	
получение привелегий пользавтеля	0,1	
получение привелегий супер пользавтеля	2	
целевой узел	0,5	
T3 = 39,6	время, ч	вероятность
старт	24	
начало атаки	5	
получение привелегий пользавтеля	0,1	
получение привелегий супер пользавтеля	10	
целевой узел	0,5	
T общ = T1*P1 + T2*P2*(1-P1) + T3*(1-P1)*(1-P2) =		33,5

Рисунок23. Граф компрометации новых интегрированных средств защиты

Время успешной атаки имеет постоянную и переменную составляющие. К первой относятся длительности разведки и нанесения ущерба, ко второй — нарушение (взлом), проникновение и эскалация. Можно предположить, что укрепление системы влияет только на переменную часть. Если постоянная часть велика, существенного снижения рисков добиться не удастся, но это означает лишь то, что система и так хорошо защищена (в эшелонированной обороне имеются хорошо укрепленные рубежи — первый и последний).

Соответственно, ориентируясь на принципы укрепления системы можно построить граф компрометации с учетом встроенных механизмов защиты, увеличивая таким образом время взлома (компрометации системы), а следовательно, минимизируя успешность действий атакующего и максимизируя успешность контрмер. Цель втираемых средств защиты и принимаемых мер в области ИБ – сохранения максимально продолжительного периода отражения угроз.

На рисунке 24 представлены примеры расчетов для приведенного графа компрометации с новыми интегрированными средствами защиты информации.

Расчеты для приведенного графа компрометации с контрмерами		
T1 = 32	время, ч	вероятность
старт	24	0,3
начало атаки	5	
получение привилегий пользователя	0,5	
получение привилегий супер пользователя	2	
целевой узел	0,5	
T2 = 32	время, ч	вероятность
старт	24	0,4
начало атаки	5	
получение привелегий пользавтеля	0,5	
получение привелегий супер пользавтеля	2	
целевой узел	0,5	
T3 = 48	время, ч	вероятность
старт	24	
начало атаки	8	
получение привилегий пользователя	0,5	
получение привилегий супер пользователя	15	
целевой узел	0,5	

Рисунок 24. Расчеты для привенного графа компрометации с новыми интегрированными средствами защиты информации

2. Практическая часть

2.1 Изучить основной теоретический материал о графе **компрометации.**

2.2 Произведите анализ угроз ИБ ИС выбранной организации, определите их класс.

2.3 По изученной методике **постройте** граф **компрометации** относительно выбранной организации, выбрав определённую проблемную область (перехват данных при файловом обмене, утечка данных через электронные почтовые сообщения, вредоносные воздействия и т. д.), определив основные параметры безопасности, требуемые для реализации методики.

2.4 По изученной методике **постройте** граф **компрометации** относительно выбранной организации, выбрав определённую проблемную область со встроенными средствами безопасности, увеличивающими период достижения цели злоумышленником максимально.

2.5 Проанализируйте графу представленные в Приложении № 2.

2.6 Сделайте выводы по результатам анализа вашей ИС.

2.7 Результаты исследования внесите в отчет.

Контрольные вопросы:

1. Дайте определения уязвимости информации, защищенности информации, угрозам безопасности информации, защите информации. Перечислите источники угроз безопасности информации.

2. Охарактеризуйте основные принципы определения экономической эффективности системы информационной безопасности.

3. Проясните положительные и отрицательные особенности методики оценки экономической эффективности системы информационной безопасности.

Практическая работа № 8. Экономическая оценка контрмер в ИБ

Программно-аппаратные средства: стандартные средства Microsoft Office.

1.Теоретический материал

Можно использовать графы атак совместно с экономической оценкой состояния защищаемого объекта со стороны защиты и со стороны атакующего [13].

Однократный ущерб на ресурс будем определять по формуле:

$$SLE = AV * EF \ , \tag{12}$$

где AV — ценность ресурса, в которую входят все виды затрат на него (установка, сопровождение и т. п.), а EF — величина стоимости объекта, утрачиваемая при успешных атаках (относительный ущерб от однократной компрометации ресурса).

Ожидаемый годовой ущерб (ARO) находится с учетом статистики инцидентов по формуле [13]:

$$ALE = SLE * ARO \ . \tag{13}$$

Оценка значения ARO может производиться на основе анализа статистики нарушений информационной безопасности.

Экономический эффект от реализации мер по защите информации (т. е. от расходов на информационную безопасность) вычисляется по формуле (14):

$$ROI = ((ALE * RM) - CSI) \setminus CSI \ , \tag{14}$$

где CSI — стоимость внедренных средств и мер защиты;

- *RM* — коэффициент уменьшения риска при установке контрмеры (лежит в промежутке от 0 до 1).

При положительном значении *ROI* защита экономически эффективна.

Экономическая эффективность действий атакующего оценивается с помощью величины *ROA*, вычисляемой по формуле [13]:

$$ROA = GI \setminus (EBS + EAS), \tag{15}$$

где *GI* — ожидаемая выгода от успешной атаки, *EBS* — затраты на компрометацию ресурса до реализации контрмеры *S*, *EAS* — дополнительные затраты на компрометацию после реализации контрмеры *S*. Цель защищающейся организации состоит в минимизации значения *ROA*, то есть в уменьшении привлекательности ресурсов организации как объектов возможных атак [13].

Угрозы успешно реализуется через уязвимости. В графах атак уязвимости ассоциируются с концевыми вершинами, т. е. вершинами, из которых не выходит ни одного ребра. С этими же вершинами ассоциируются контрмеры, ликвидирующие или уменьшающие уязвимости [13].

Граф атаки строится с использованием логических операций *И, ИЛИ* (когда достаточно одного из нескольких условий - связка *ИЛИ,* когда требуется одновременное выполнение условий используется связка И). Преобразование к дизъюнктивной нормальной форме основывается на логическом тождестве: *(А ИЛИ В) И С = (А И С) ИЛИ (В И С)*.

Рассмотрим пример компрометации конфиденциальных данных путем кражи сервера, на котором они хранятся (рисунок 24). Чтобы украсть сервер, нужно сначала проникнуть в серверную комнату, а затем незаметно вынести сервер. Чтобы проникнуть в серверную комнату, можно взломать дверь или раздобыть (подобрать) ключи (Рисунок 25).

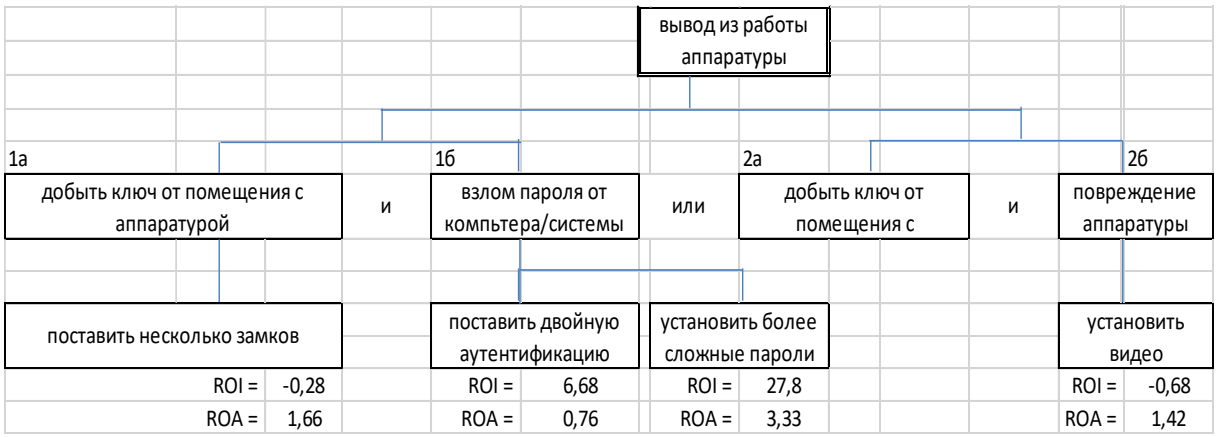


Рисунок 25. Фрагмент графа атак, аннотированного контрмерами и показателями экономической эффективности.

Чтобы противодействовать всем возможным (идентифицированным) атакам необходимо установить регуляторы безопасности на каждом пути в графе атак от концевых вершин к целевой (точнее как минимум одна контрмера нужна для каждой связки И), отдавая предпочтение контрмерам с максимальным значением *ROI*.

Если один регулятор безопасности противодействует нескольким атакам, затраты на него следует поделить поровну между соответствующими вариантами атак (рисунок 26).

1а		1б		2а			2б
AV	20000	AV	20000	AV	20000	AV	20000
EF	0,9	EF	0,6	EF	0,6	EF	0,9
SLE	**18000**	**SLE**	**12000**	**SLE**	**12000**	**SLE**	**18000**
ARO	0,5	ARO	0,8	ARO	0,8	ARO	0,3
ALE	**9000**	**ALE**	**9600**	**ALE**	**9600**	**ALE**	**5400**
RM	0,2	RM	0,8	RM	0,3	RM	0,6
CSI	2500	CSI	1000	CSI	100	CSI	10000
ROI	**-0,28**	**ROI**	**6,68**	**ROI**	**27,8**	**ROI**	**-0,676**
GI	5000	GI	5000	GI	5000	GI	5000
EBS	2500	EBS	500	EBS	500	EBS	3000
EAS	500	EAS	6000	EAS	1000	EAS	500
ROA	**1,6667**	**ROA**	**0,769230769**	**ROA**	**3,333333**	**ROA**	**1,428571**

Рисунок 26. Данные к графу атаки

Анализ экономической эффективности контрмер для *ROA* проводится сходным с *ROI* образом, только значение *ROA* следует не максимизировать, а минимизировать (атаки на ресурсы организации должны иметь для злоумышленника минимальную привлекательность). Если одновременная максимизация *ROI* и минимизация *ROA* невозможны, для осуществления выбора регуляторов безопасности необходимо привлечь дополнительные соображения.

2. Практическая часть

2.1 Изучить основной теоретический материал о **графе атаки.** Рассмотрите материал в Приложении № 3.

2.2 Произведите анализ угроз ИБ ИС выбранной организации, определите их класс.

2.3 По изученной методике **постройте** граф **атаки** относительно выбранной организации, выбрав определённую проблемную область (перехват данных при файловом обмене, утечка данных через электронные почтовые сообщения, вредоносные воздействия и т. д.), определив основные параметры безопасности, требуемые для реализации методики.

2.4 По изученной методике **постройте** граф **атаки** относительно выбранной организации, выбрав определённую проблемную область со встроенными средствами безопасности, увеличивающими период достижения цели злоумышленником максимально.

2.5 Проанализируйте графу представленные в приложении 3.

2.6 Реализуйте экономические расчеты при решении задач построения графа атаки.

2.7 Сделайте выводы по результатам анализа вашей ИС.

2.8 Результаты исследования внесите в отчет.

Контрольные вопросы:

1. Дайте определения уязвимости информации, защищенности информации, угрозам безопасности информации, защите информации в методики **графа атаки**.

2. Охарактеризуйте основные принципы построение **графа атаки**.

3. Проясните положительные и отрицательные особенности методики оценки уязвимости информации.

ЗАКЛЮЧЕНИЕ

Правильная организация практических учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 г. N 373-ст: дата введения 2008-02-01. – URL: https://docs.cntd.ru/document/1200058320 (дата обращения: 15.04.2021). – Текст: электронный.

2. ГОСТ Р ИСО 19011-2012. Руководящие указания по аудиту систем менеджмента: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 19 июля 2012 г. N 196-ст: дата введения 2013-02-01. – URL:

https://docs.cntd.ru/document/1200095049 (дата обращения: 15.04.2021). – Текст: электронный.

3. Аудит информационной безопасности органов исполнительной власти: учебное пособие / В. И. Аверичников, М. Ю. Рытов, А. В. Кувылкин, М. В. Рудановский. – Москва: Флинта, 2011. – 100 с. – ISBN 978-5-9765-1277-1.

4. Аверченков, В. И. Оптимизация выбора состава средств инженерно-технической защиты информации на основе модели Клементса-Хоффмана / В. И. Аверченков, М. Ю. Рытов, Т. Р. Гайнулин // Вестник Брянского государственного технического университета. – 2008. – №1. – С. 61-66.

5. Аверченков, В. И. Аудит информационной безопасности: учеб. пособие для вузов / В. И. Аверченков. – 2-е изд., стер. – Брянск: БГТУ, 2010. – 268 с. – ISBN 978-89838-487-6.

6. Аверченков, В. И. Аудит информационной безопасности: учеб. пособие для вузов / В. И. Аверченков. – 3-е изд., стер. – Москва: Флинта, 2016. – 269 с. – ISBN 978-5-9765-1256-6.

7. Банк данных угроз безопасности информации: официальный сайт. – URL: https://bdu.fstec.ru/scanoval (дата обращения: 15.05.2021). – Текст: электронный.

8. Колегов Д. Н. Проблемы синтеза и анализа графов атак [Электронный ресурс]. Режим доступа: http://www.securitylab.ru

9. Котенко, И. В. Многоагентные технологии анализа уязвимостей и обнаружения вторжений в компьютерных сетях / И. В. Котенко // Новости искусственного интеллекта. – 2004. – № 1. – С. 56–72.

10. Джексон, П. Введение в экспертные системы / П. Джексон.- Москва: Вильямс, 2001. – 624 с.

11. Люгер, Д. Ф. Искусственный интеллект, стратегии и методы решения сложных проблем [Текст]/ Д. Ф. Люгер. – 4-е изд. – Москва: Вильямс, 2003. – 864 с.

12. Schneier B. Attack Trees. – Dr. Dobbs Journal, December 1999.

13. Управление рисками: обзор употребительных подходов //Jet Info, № 12, 2006 г.

14. Мониторинг и аудит информационной безопасности автоматизированных систем / В. В. Кульба, А. Б. Шелков, Ю. М. Гладков, С. В. Павельев. – Москва: ИПУ им. В.А. Трапезникова РАН, 2009. – 94 с. – ISBN 5-201-15025-8.

15. Макаренко, С. И. Аудит безопасности критической инфраструктуры специальными информационными воздействиями: монография / С. И. Макаренко. – Санкт-Петербург: Наукоемкие технологии, 2018. – 122 с. – ISBN 978-5-6041427-8-3.

16. Nmap network scaning: официальный сайт. – URL: https://nmap.org/book/ (дата обращения: 18.05.2021). – Текст: электронный.

17. Организация аудита информационной безопасности: сайт – URL: https://accounting.fa.ru/jour/article/viewFile/129/130.pdf (дата обращения: 22.05.2021). – Текст: электронный.

18. Различные приемы сканирования портов: сайт. – URL: https://nmap.org/man/ru/man-port-scanning-techniques.html (дата обращения: 15.05.2021). – Текст: электронный.

19. Сканер уязвимостей Nessus: сайт. – URL: https://networkguru.ru/tenable-nessus-vulnerability-scanner/ (дата обращения: 20.05.2021). – Текст: электронный.

20. Сканер уязвимостей XSpider: сайт. – URL: http://www.s-t.ru/2014-03-16-16-26-58/237--xspider.html (дата обращения: 22.05.2021). – Текст: электронный.

21. Хомяков, В. А. Аудит как метод модернизации системы обеспечения информационной безопасности / В. А. Хомяков // Экономический вестник Ярославского университета. – 2013. – № 29. – С. 48-52.

Приложение №1. Дерево угроз и уязвимостей

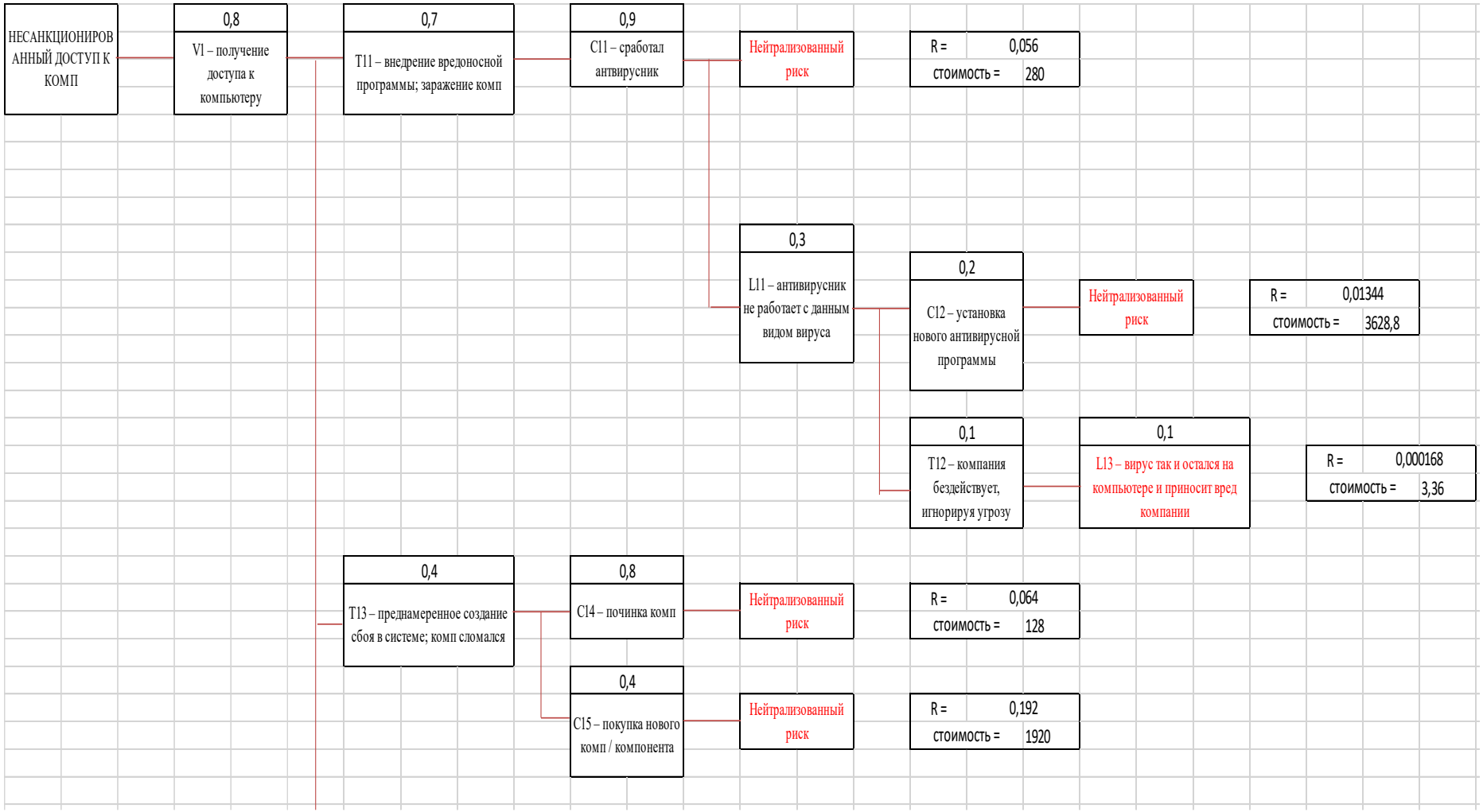
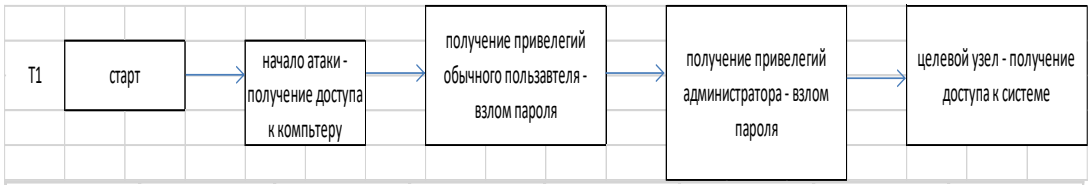


Рисунок 1. Дерево угроз и уязвимостей

Приложении № 2. Фрагмент графа компрометации и расчеты

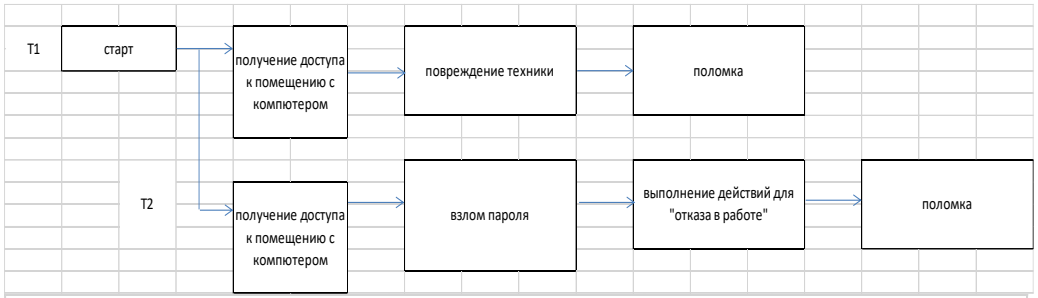
1. НСД к системе



без контрмер		
T1 = 38,5	время, ч	вероятность
старт	24	0,4
начало атаки	3	
получение привелегий пользавтеля	5	
получение привелегий супер пользавтеля	6	
целевой узел	0,5	
T общ = T1*P1 =		15,4

Рисунок 1. Фрагмент графа компрометации и расчеты

2.Повреждение аппаратуры



без контрмер			
T1 = 31,1		время, ч	вероятность
старт		24	0,8
начало атаки		6	
получение привелегий пользавтеля		0	
получение привелегий супер пользавтеля		1	
целевой узел		0,1	
T2 = 37,1		время, ч	вероятность
старт		24	0,3
начало атаки		6	
получение привелегий пользавтеля		3	
получение привелегий супер пользавтеля		4	
целевой узел		0,1	
T общ = T1*P1 + T2*P2*(1-P1)			27,106

Рисунок 2. Фрагмент графа компрометации и расчеты

Приложение № 3. Фрагмент графа атаки и расчеты

1.Атака «Кража документов»

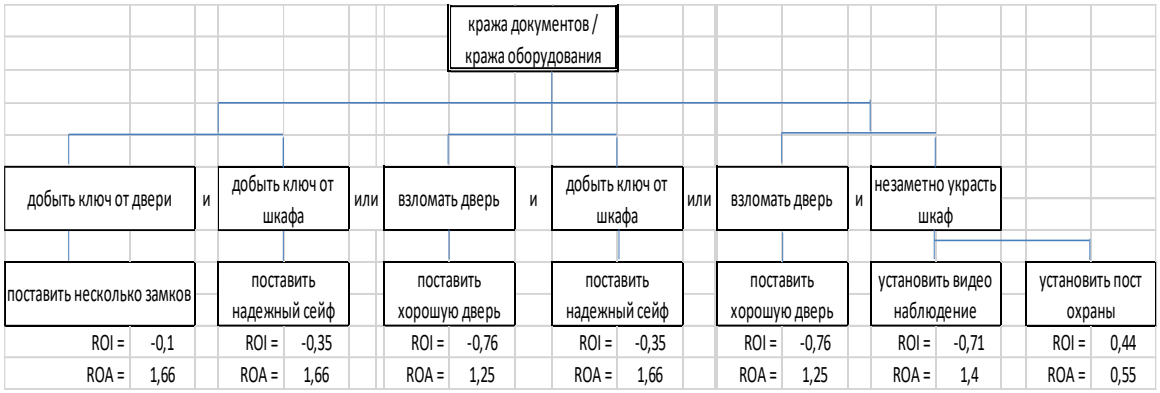


Рисунок 1. Фрагмент графа атаки и расчеты

Локальный электронный методический материал

Владислав Владимирович Подтопельный

АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Редактор Г. А. Смирнова

Уч.-изд. л. 3,75. Печ. л. 3,75

Издательство федерального государственного бюджетного образовательного
учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1

60