МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ
ОБРАЗОВАТЕЛЬНОЕУЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «Организационно-правовое обеспечение информационной безопасности»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль)
«Информационная безопасность киберфизических систем»

Ставрополь
2026 г.

СОДЕРЖАНИЕ

Введение

Целью освоения дисциплины «Организационно-правовое обеспечение информационной безопасности» является формирование профессиональной компетенции будущего магистра по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Информационная безопасность киберфизических систем» для осуществления деятельности в области защиты киберфизических систем, а также создания новых объектов киберфизических систем, а также теоретическая и практическая подготовленность магистра для проведения работ по обеспечению организационной и правовой безопасности информации в соответствии с современными требованиями.

Основными задачами дисциплины является:

– изучение основ правового регулирования отношений в информационной сфере, конституционных гарантий прав граждан на получение информации и механизмы их реализации;

– изучение основных понятий и видов защищаемой информации, согласно законодательству РФ;

– изучение основ правового регулирования отношений в области государственной тайны, конфиденциальной информации и интеллектуальной собственности, методов и способов защиты такой информации;

– изучение сущности и содержания организационных мероприятий по защите информации;

– обучение студентов основам расследования преступлений в информационной и компьютерной сферах;

– приобретение студентами знаний, умений и практических навыков по правовому и организационному обеспечению защиты информации.

Дисциплина «Организационно-правовое обеспечение информационной безопасности» (Б1.В.04) относится к дисциплинам части, формируемой участниками образовательных отношений. Её освоение происходит в 1 семестре.

Компетенции обучающегося, формируемые в результате освоения дисциплины

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине, характеризующие этапы формирования компетенций, индикаторов
ПК-3 Способен разрабатывать предложения по совершенствованию системы управления информационной	ИД-1 ПК-3 состав, порядок функционирования и алгоритм построения системы управления информационной безопасностью киберфизических систем	Имеет понимание состава и порядка функционирования системы управления информационной безопасностью киберфизических систем

безопасностью киберфизических систем	ИД-2 ПК-3 анализ уязвимости и построение модели угроз для киберфизических систем	Умеет строить модель угроз для киберфизических систем
	ИД-3 ПК-3 выбора и реализации набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем	Владеет навыками реализации набора организационно-технических и криптографических мер в системе информационной безопасности киберфизических систем
	ИД-4 ПК-3 осуществляет анализ предложений по совершенствованию системы управления информационной безопасностью киберфизических систем	Перечисляет и кратко характеризует основные нормативные документы, определяющие требования к системе управления информационной безопасностью киберфизических систем

Практическая работа № 1

Тема. Государственная система защиты информации Российской Федерации

Цель занятия: Научиться устанавливать и настраивать все компоненты системы на отдельном сервере. Усвоить порядок установки компонентов.

Теоретическая часть:

Программный продукт MaxPatrol 10 приходит на смену предыдущему программному продукту компании Positive Technologies – MaxPatrol 8 и призван расширить функционал хорошо известной системы анализа защищенности и контроля соответствия стандартам. Программное обеспечение, призванное защитить инфраструктуру предприятия от компьютерных атак, чрезвычайно разнообразно. Чтобы ориентироваться в функциях защитного ПО, мы можем выделить такие защитные механизмы, как:

1. Превентивные.
2. Детективные.
3. Коррективные.

Так же в терминах времени, мы можем представить ландшафт типичной атаки как действия, предпринимаемые злоумышленником до атаки, во время и после нее. Для того, чтобы полноценно противодействовать злоумышленнику в рамках концепции эшелонированной защиты, необходимо понимать ландшафт атаки, понимать устройство информационной системы и иметь возможность предпринимать защитные меры в любой точке информационного пространства и в любой точке временного ландшафта.

До начала атаки злоумышленник, как правило, собирает информацию об атакуемой системе. Строго говоря, это необязательная стадия, так, вирусные эпидемии, распространение RansomWare (шифровальщиков-вымогателей) обходится без разведки. Тем не менее, есть некоторая деятельность, обнаружение которой может свидетельствовать (но не обязательно) о подготовке злоумышленника к атаке. Сюда можно отнести:

1. Сбор информации с веб-сайта (crawling) с использованием словарей.
2. Сбор fingerprint’ов операционных систем и сервисов.
3. Сканирование сетей и портов.

В процессе атаки злоумышленник эксплуатирует известные ему уязвимости (тут надо понимать, что уязвимость может быть не только следствием ошибки реализации программного обеспечения, но и следствием ошибки проектирования ПО или информационной системы и следствием ошибки эксплуатации), осуществляет DoS и DDoS атаки, пытается проникнуть в систему при помощи отправки фишинговых писем или просто спама.

И наконец, после того как атака проведена, злоумышленнику надо закрепиться в системе. Цель злоумышленника необязательно состоит в том, чтобы причинить зримый вред атакованному объекту. Напротив, работающий подконтрольный злоумышленнику ресурс может быть намного более ценен, чем выведенный из строя. Внедренное malware может годами ждать своего

часа или причинять ущерб третьим лицам, подставляя в качестве источника атаки скомпрометированные системы.

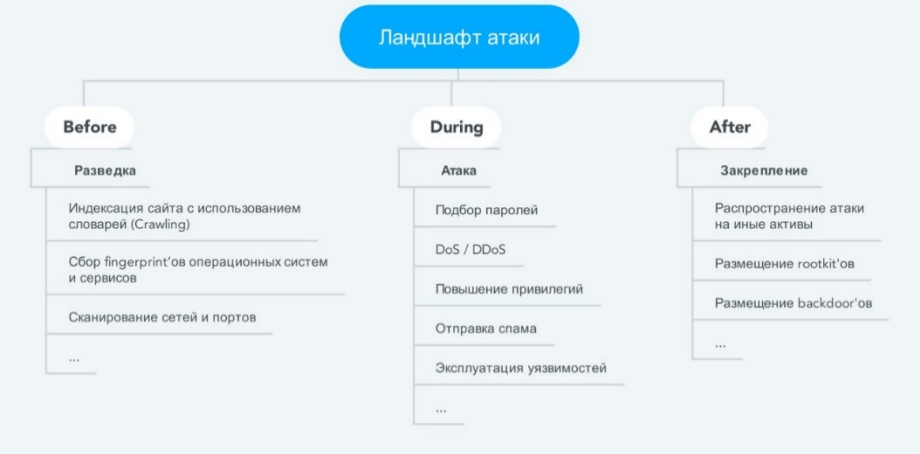


Рисунок 1.1 – Ландшафт атаки

На каждом этапе ландшафта атаки, злоумышленник может столкнуться с теми или иными защитными мерами. О сканировании системы администратора, может быть, предупредит система обнаружения вторжений (СОВ или IDS). Об атаке может предупредить (а может быть даже предотвратит) та же IDS или антивирусное средство. Всё это детективные меры защиты, они безусловно важны, но недостаточны для выстраивания эшелонированной защиты.

Для выстраивания полноценной эшелонированной защиты администратор, в первую очередь, должен понимать, как устроена его информационная система: какие в ней есть активы (реальные и виртуальные хосты, веб-сервисы), какие операционные системы ими управляют, какие сервисы и какое программное обеспечение там имеется. В идеальном случае каждый процесс, которому есть что рассказать о конфиденциальности, целостности и доступности предоставляемых сервисов, должен быть известен администратору ИБ равно как и связи между ними. Для приоритизации усилий администратор ИБ должен понимать степень критичности вверенных ему активов, допустимое время простоя или другой подобный параметр. При этом не надо забывать о том, что люди (работники предприятия, партнеры, клиенты, контрагенты) тоже являются частью информационной системы и несут определенные специфические риски для нее. Учет совокупности информационных активов называется управлением активами или Asset Management и сам по себе он уже является важной превентивной мерой защиты информационной системы.

Следующий шаг - это выстраивание процесса управления уязвимостями или Vulnerability Managment (VM). В рамках этого процесса администратор выстраивает регулярные циклические процедуры обнаружения дефектов в области безопасности информационной системы (обнаружение уязвимостей, ошибок эксплуатации, несовершенства дизайна сети и т.п.), исправления обнаруженных проблем, верификации результатов, планирования

последующих действий. Создание такого процесса – важнейшая превентивная мера защиты.

В процессе атаки или во время разведки злоумышленник будет взаимодействовать с различными объектами информационной системы. Эта деятельность не должна пройти незамеченной. На предварительном этапе анализа администратор ИБ должен был не только осознать схему информационной системы, но и получить возможность анализа сообщений от каждого ее элемента. Сбор, хранение и обработка журнальной информации, касающейся конфиденциальности, целостности и доступности сервисов предприятия, – так же важный процесс в составе эшелонированной защиты. На этот раз мы говорим о детективных мерах, этот процесс называется управлением событиями безопасности или Security Information and Event Management (SIEM).

Наконец, после того как атака завершилась (а иногда даже до того, как будет проведено восстановление из резервной копии) наступает новый важный этап – расследование или Forensic. Расследование необходимо для того, чтобы понять, как проник в систему злоумышленник и что он успел в ней предпринять. Какие активы потенциально могли быть доступны ему кроме тех, на которых его деятельность была обнаружена. Данный набор мер относится к коррективным мерам. Сведения, которые оказываются в распоряжении администратора ИБ по итогам расследования инцидента, не только влияют на реагирование на инцидент (проверка потенциально скомпрометрированных активов), но и попадают на вход уже запущенного процесса VM (сведения о способе проникновения злоумышленника в систему).

Важно понимать, что в приведенной концепции работа всех компонентов является тесно взаимосвязанной. Обратная связь от процесса Forensic к процессу Vulnerability Management здесь не единственная. Так процессы AssetManagment’а должны обогащаться данными от работы модулей сбора событий, актуализируя информацию об активах. И наоборот, система анализа событий обогащается данными об активах для того, чтобы принимать более точные решения. Информация об активах необходима для анализа событий с учетом ролей узлов, их критичности и имеющихся на них уязвимостях и других особенностей.

Рисунок 1.2 – Защитные меры в рамках концепции MaxPatrol 10

При этом ключевая задача, которую должна решать система MaxPatrol 10, состоит в том, чтобы не только предоставить администратору ИБ возможность самостоятельно заниматься перечисленными процессами, но и привнести в этот процесс экспертизу исследовательского центра Positive Technologies. Трудно представить, что в реальных условиях найдется достаточное количество специалистов, обладающих необходимым объемом знаний обо всех элементах информационной системы.

Задача создания программного обеспечения, которое бы смогло полностью реализовать представленную концепцию, очень сложна. Её реализация требует не только большой экспертизы в области информационной безопасности, но и эффективной работы с чрезвычайно большими объемами данных в реальном времени. В настоящее время мы представляем вашему вниманию программный продукт MaxPatrol 10 SIEM Edition, который решает задачи сбора, хранения и анализа событий, а также задачи Asset Management'а и Vulnerability Management'а, в той части, в которой они необходимы для работы системы SIEM.

Методические рекомендации по выполнению практического занятия

1. На машине Core_XX (логин Administrator, пароль P@ssw0rd) зайдите в каталог C:\Users\Administrator\Downloads\MPXDeployment.18.0.2006, найдите файл MPXCoreSetup_18.0.2006.exe (версия может быть другой) и запустите установку компонента Core. Установка занимает длительное время, в процессе установки понадобится перезагрузка узла. (Ориентировочное время на установку 10 минут до перезагрузки и 25 после.) Рекомендацию не устанавливать продукт на системный диск проигнорируйте.

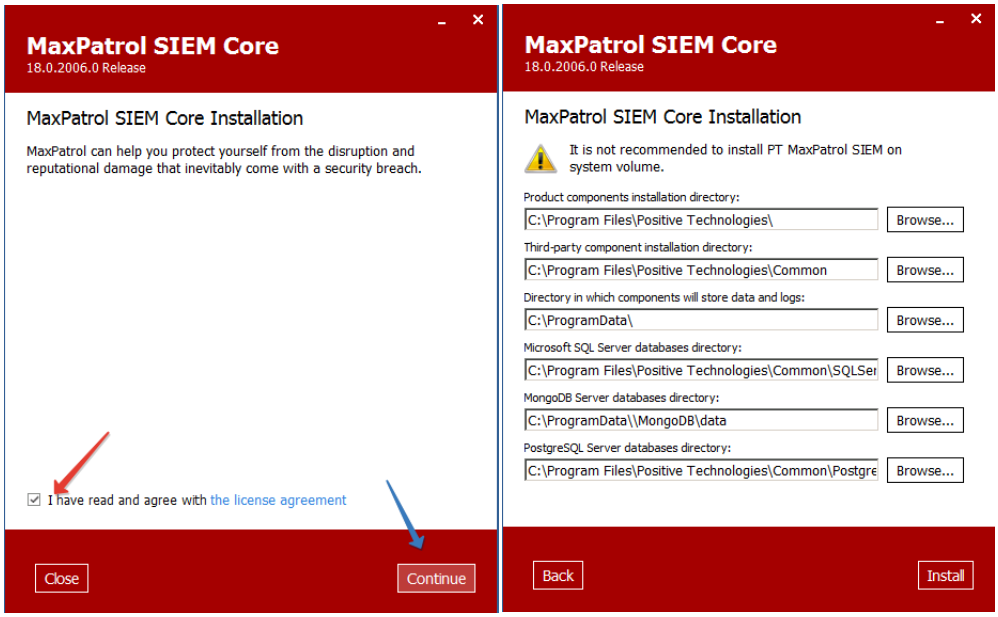


Рисунок 1.3 – Этап установки

2. Аналогично из папки C:\Users\Administrator\Downloads\MPXDeployment.18.0.2006 запустите установку MPXSiemSetup_18.0.2006.exe (5 минут).

3. И наконец, установите третий компонент – MPXAgentSetup_18.0.2006.exe (2 минуты).

4. Скопируйте файл gnclient.ini из места, указанного преподавателем (например, Courseware for students\PT13 - SIEM\License на рабочем столе сервера RDS), на машину core-XX в папку C:\ProgramData\Positive Technologies\MaxPatrol SIEM Core\Config

После завершения установки всех необходимых компонентов, их необходимо сконфигурировать для совместной работы. Для этого выполните следующие шаги:

5. На машине Core_XX в командной строке отдайте команду mpxcore get. Если команда не срабатывает, перейдите в каталог C:\Program Files\Positive Technologies\MaxPatrol SIEM Core\.install или просто заново авторизуйтесь в системе.

C:\Users\Administrator>mpxcore get HostAddress = 'localhost' (String) SiemAddress = 'localhost' (String)

...

Аналогично можно управлять настройками компонентов SIEM и Agent при помощи команд mpxsiem и mpxagent. Команда mpxcore предназначена не только для просмотра конфигурационных параметров, но и для их изменения. После изменения конфигурационных файлов, команда mpxcore перезапускает сервисы, это довольно длительный процесс, поэтому нам надо изменить необходимые опции за одно действие для этого сохраним все опции в конфигурационный файл, отредактируем его и применим.

6. Отдайте команду

C:\Users\Administrator>mpxcore get –f Desktop\mpxcore.xml

7. Откройте файл mpxcore.xml текстовым редактором и удалите или

закомментируйте (<--! Это многострочный комментарий в XML -->) опции SSLCertificateThumb и DataVersion. Можно удалить вообще все опции кроме тех, которые нам необходимо изменить (см. ниже), но необходимости в этом нет.

8. В опциях HostAddress и PtkbFeatureHost напишите core-XX.edu.ptsecurity.com

(где XX номер вашего стенда с нулем, например 05).

9. Сохраните файл и отдайте команду

C:\Users\Administrator>mpxcore set –f Desktop\mpxcore.xml

 Внимание! Это действие может занять неожиданно много времени. Утилита mpxcore не только модифицирует конфигурационные файлы, но также и перезапускает службы. Пожалуйста дождитесь успешного перезапуска служб.

 Более полная информация о настройке системы приведена в документации, см. ptmpsiem18.0_adminguide_ru.pdf в каталоге Courseware for Students. Вопросы установки системы также подробно изложены в углубленном курсе по MaxPatrol SIEM. Если у вас есть какие-то вопросы, касающиеся этого материала, вы можете задать их непосредственно преподавателю.

10. Аналогично создайте конфигурационный файл mpxptkb.xml:

C:\Users\Administrator>mpxptkb get –f Desktop\mpxptkb.xml

11. Откройте файл mpxptkb.xml текстовым редактором и удалите или закомментируйте (<--! Это многострочный комментарий в XML -->) опции SSLCertificateThumb и EnableWebUI. Можно удалить вообще все опции кроме тех, которые нам необходимо изменить (см. ниже), но необходимости в этом нет.

12. В опциях HostAddress, IdentityServerAddress и CoreAddress напишите core- XX.edu.ptsecurity.com (где XX номер вашего стенда с нулем, например 05).

13. Сохраните файл и отдайте команду

C:\Users\Administrator>mpxptkb set –f Desktop\mpxptkb.xml

14. Откройте в браузере (поддерживаются браузеры Chrome, Firefox и Internet Explorer старше 11-го) интерфейс MaxPatrol SIEM с машины RDS по адресу установленному в пункте 6 (http://core-XX.edu.ptsecurity.com). Вы будете автоматически перенаправлены на страницу авторизации. Введите логин и пароль Administrator/P@ssw0rd

15. Откройте вкладку Система/Управление системой/Агенты. Если на вкладке отображается подключенный к системе агент, то связь между агентом и ядром работает корректно.

16. Там же, на вкладке Система/Управление системой/Лицензии проверьте, наличие лицензии.

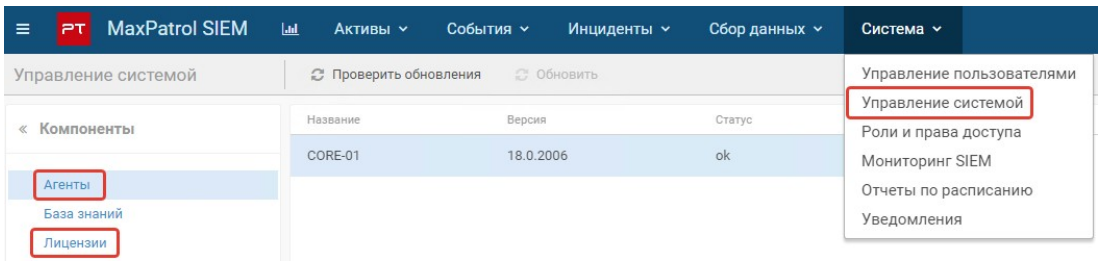


Рисунок 1.4 – Наличие лицензии

В верхней панели интерфейса справа имеется значок системы Health Monitoring. Он может быть либо красным, либо зеленым. В обоих случаях щелчек по нему выводит окошко с перечнем имеющихся проблем или сообщением, что проблем нет. Health Monitoring может отставать от актуальной ситуации и показывать информацию о появившейся лицензии спустя некоторое время (до пяти минут). Клик по значку Health monitor заставляет его перечитать информацию.

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

Отчет должен включать:

– титульный лист;

– цель работы;

– ход работы, содержащий пошаговое описание осуществленных действий, иллюстрированных скриншотами на каждом этапе выполнения;

– вывод.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Практическая работа № 2

Тема. Организационные системы обеспечения безопасности информации

Цель занятия: Научиться создавать задачи на сканирование, при помощи журнала сканирования научиться понимать реальные действия, проделанные системой. Усвоить, где находятся журналы агента.

Теоретическая часть:

Функциональные возможности текущей версии MaxPatrol SIEM

Функциональные возможности MaxPatrol позволяют организовать цикл работы с событиями безопасности, который включает в себя следующие этапы:

1. Сбор событий от разных внешних источников. В стандартный комплект поставки MaxPatrol SIEM входит поддержка следующих форматов и протоколов:

- Syslog – пассивный сбор событий по протоколу Syslog;
- Windows Event Log – активный сбор событий Windows Event log;
- Windows File log – активный сбор событий из файлов Microsoft Windows;
- Windows WMI log – активный сбор событий Windows Event log через WMI;
- NetFlow – пассивный сбор событий по протоколу NetFlow;
- ODBC Log – активный сбор событий из таблиц СУБД;
- SSH File Log – активный сбор событий из файлов по протоколу SSH;
- CheckPoint LEA – сбор информации от устройств Check Point по протоколу OPSEC;
- SNMP Traps – пассивный сбор данных по протоколу SNMP.

Система поддерживает разбор сообщений в текстовом формате, а также в форматах JSON и XML. Специалисты Positive Technologies при проведении пилотных проектов и внедрений реализуют поддержку любых нестандартных источников данных, используемых заказчиком.

2. Нормализация событий для приведения их к общему стандарту и подготовке к дальнейшей обработке.

Каждое «сырое» событие проходит через сервис нормализации и порождает нормализованное событие. Формулы нормализации можно редактировать, что позволяет реализовать поддержку практически любого источника.

3. Агрегация – удаление и объединение повторяющихся событий для сокращения объема хранения.

4. Корреляция – анализ взаимосвязей между различными событиями по заданным правилам и автоматическое создание инцидентов при срабатывании правил. Подробнее возможности по корреляции будут описаны далее.

5. Хранение – ведение архива событий и срезов состояний наблюдаемых систем для проведения глубокого анализа и расследования возможных инцидентов безопасности.

Корреляция событий безопасности – одна из основных функций SIEM-систем. С помощью правил корреляции система может приходить к обобщающим выводам относительно того, что происходит в информационной системе. Корреляция позволяет снизить нагрузку на специалистов информационной безопасности, позволяя им сосредоточиться только на важных событиях. Правила корреляции и средства их разработки входят в состав продукта.

Особенностью MaxPatrol SIEM является работа с учетом активов информационной системы заказчика. MaxPatrol SIEM автоматически собирает информацию об ИТ-инфраструктуре, строит схему (топологию) сети, анализирует версии операционных систем и установленное программное обеспечение, проводит сканирование портов и служб. Все это позволяет не только лучше анализировать возникающие инциденты и оценивать их с

привязкой к схеме сети и конкретным активам, но и снизить число ложных срабатываний за счет сопоставления событий с текущими параметрами узлов.

Методические рекомендации по выполнению практического занятия

Часть 1. Создание задачи по обнаружению узлов в сети

1. На вкладке Сбор данных/Задачи создайте задачу «Who is there?». Заполните следующие поля:

Название задачи	Who is there?
Цели сканирования/Сетевые адреса	Локальная сеть (например, 10.0.1.0/24)
Профиль	HostDiscovery

2. Нажмите кнопку «Сохранить и запустить» (рисунок 2.1).

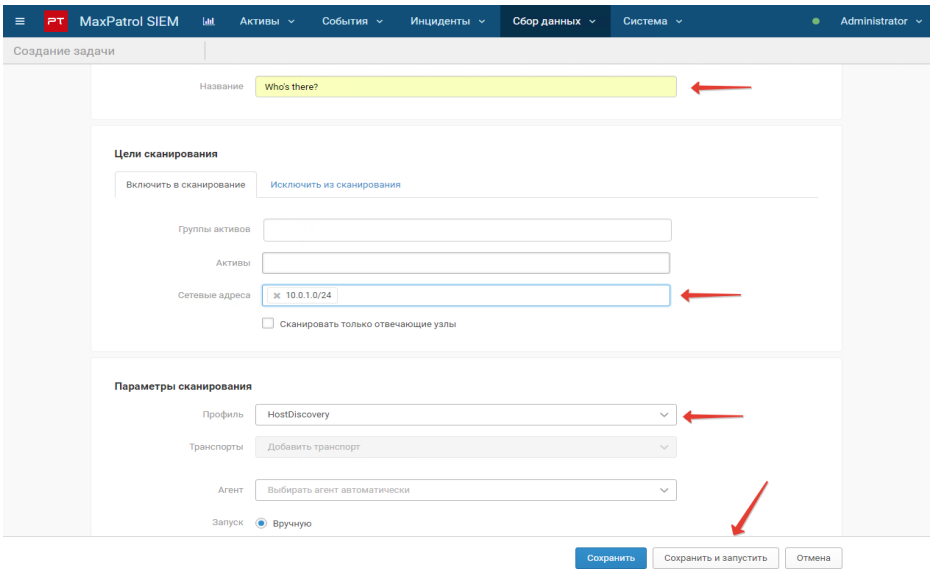


Рисунок 2.1 – Кнопка «Сохранить и запустить»

3. В процессе выполнения задачи системой ее статус «Выполняется» будет виден в правой части экрана. По завершении задачи он изменится на «Выполнена без ошибок» (понадобится обновить страницу или переключиться по ссылкам Все задачи/запущенные или перезагрузить станицу).

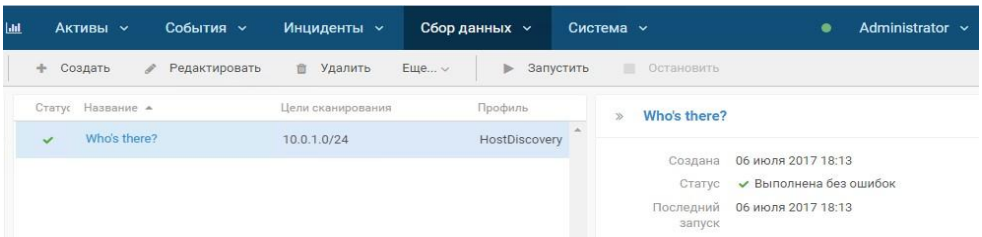


Рисунок 2.2 – Сбор данных

По мере выполнения задачи на вкладке Активы/Конфигурация в системной группе Unmanaged hosts должны появляться активы.

4. Изучите журналы агента через пользовательский интерфейс: пройдите внутрь задачи и скачайте журнал. Так же найдите журнал сканирования на агенте в папке C:\ProgramData\Positive Technologies\MaxPatrol SIEM Agent\log\<имя модуля>\.

5. Аналогичным способом создайте задачи «Where Windows?» и «Port Scan». На этот раз дополнительно задайте опцию «Сканировать только отвечающие узлы»:

Название задачи	Where Windows?
Цели сканирования/Сетевые адреса	Локальная сеть (например, 10.0.1.0/24)
Профиль обнаружения узлов	HostDiscovery
Профиль	Windows Discovery

Во время сканирования вы можете кликнуть по имени задачи на вкладке «Сбор данных/Задачи» и увидеть список подзадач с возможностью скачать журнал сканирования по каждой из них.

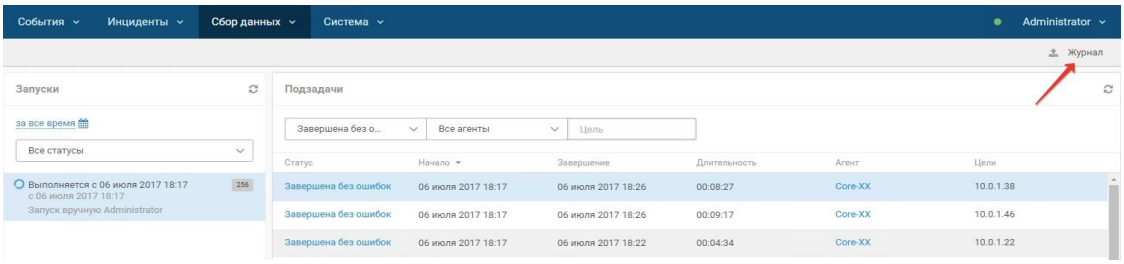


Рисунок 2.3 – Сбор данных/Задачи

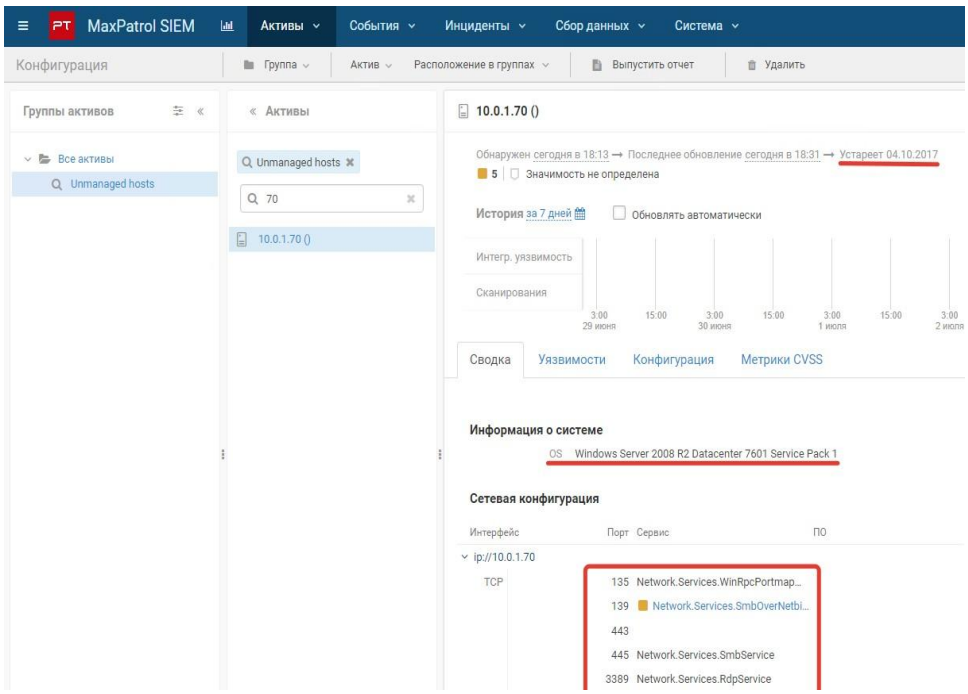


Рисунок 2.4 – Информация о системе

Обратите внимание, что на вкладке с Активами в результате работы профиля у узлов под управлением Microsoft Windows появилось название операционной системы и определились прослушиваемые порты.

Часть 2. Создание групп активов

Цель: Научиться создавать статические и динамические группы активов.

1. Создайте статическую группу Example. Группа будет располагаться в корне иерархии.

Название	Example
Тип группы	Другая
Расположение	Root

2. В группе Example создайте динамическую группу Windows. Укажите группе расположение Example и добавьте фильтр активов Core.Host/OsName Windows.

Название		Windows
Расположение		Example
Фильтр	WHERE	WindowsHost

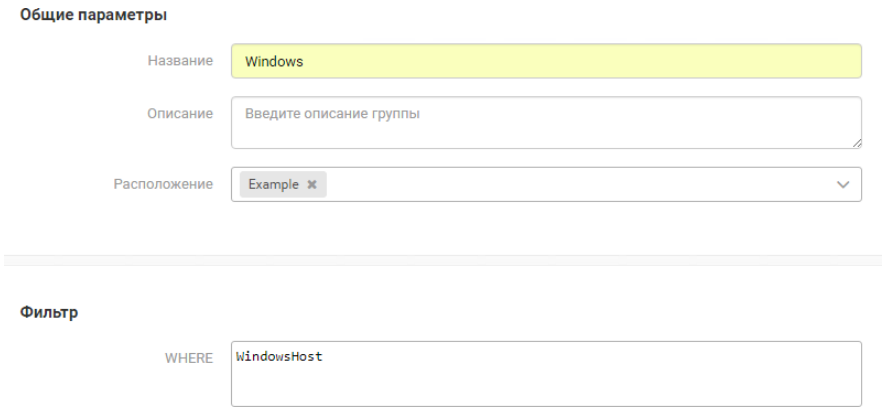


Рисунок 2.5 – Группа, расположение, фильтр

3. В группе Example создайте динамическую группу Linux. Укажите группе расположение Example и добавьте фильтр активов Host.Endpoints<TransportEndpoint>[Status = 'Open' and Protocol = 'tcp' and Port = 111]. Мы пока еще не проводили аудита Linux. Поэтому заполняем группу узлами, у которых открыт порт 111. После Аудита можно будет отредактировать Фильтр активов упростив его до простого выражения LinuxHost. Конечно, переписать столь длинное выражение без ошибок не просто. Для составления выражения удобно воспользоваться конструктором выражений PDQL. Эта тема подробнее будет освещена далее в разделе «Динамические группы. Язык запросов PDQL».

Название	Linux (111)

Расположение		Example
Фильтр	WHERE	Host.Endpoints<TransportEndpoint>[Status = 'Open' and Protocol = 'tcp' and Port = 111]

Аналогично можно создать динамические группы для поиска узлов с определенным ПО или решить иные задачи.

Часть 3. Аудит Windows и Linux, сбор событий

Цель: Научиться создавать учетные записи для авторизации в Windows и Linux, для повышения привилегий в Linux. Научиться повышать привилегии при помощи команды su. Результаты работы задачи FastPentest понадобятся в дальнейших работах.

1. На вкладке Сбор данных/Учетные записи создайте учетную запись типа логин-пароль для аудита Windows.

Название учетной записи	Windows Auditor
Транспорты	SMB / Windows audit / Windows logs
Логин	Administrator
Пароль	P@ssw0rd

2. Аналогично создайте две учетные записи для аудита Linux. Одна учетная запись понадобится для входа в систему (вход под учетной записью root заблокирован). Вторая понадобится для повышения привилегий.

Название учетной записи	Linux Auditor 1
Транспорты	Terminal
Логин	yoda
Пароль	P@ssw0rd

Название учетной записи	Linux Auditor 2
Транспорты	Terminal
Логин	root
Пароль	P@ssw0rd

3. Создайте и запустите задачу Windows Audit. На этот раз в качестве целей сканирования укажем не локальную сеть, а группу активов Windows – результат работы предыдущих задач.

Название задачи		Windows Audit
Цели сканирования	Группы активов	динамическая группа Windows
Профиль		Windows Audit
Учетная запись		Windows Auditor

4. Теперь создайте и запустите задачу по аудиту Linux. Задачу создаем аналогичным образом, но на этот раз нам понадобится выполнить дополнительные настройки транспорта. Для этого следует в диалоге создания

задачи нажать значок с «шестеренкой» и в параметрах транспорта выполнить следующие две настройки:

Тип локальной аутентификации Local authorization method	1
Метод повышения привилегий Privilage escalation method	1

Или перейти на вкладку JSON и в нижнем окне переопределить два Параметра:

```
{
"SSH.AUTH_TYPE": 1,
"SSH.USE_ROOT_LOGON_TERMINAL": 1
}
```

В Таблице 2.1 для справки приведены значения параметров повышения привилегий транспорта Terminal.

Таблица 2.1 – Опции транспорта Terminal, предназначенные для повышения привилегий

SSH.TERMINAL_SYSTEM_TYPE	Тип терминала	0-Unknown 1-Autodetect 2-Unix 3-Cisco 4-Checkpoint 5-Netware
SSH.AUTH_TYPE	Тип повышения привилегий	0-None 1-Unix (su) 2-Cisco (enable) 3-checkpoint (expert) 4-использовать команду, заданную в параметре SSH.CUSTOM_AUTH
SSH.USE_ROOT_LOGON_TERMINAL	Метод повышения привилегий	0-Не повышать привилегии 1-Повысить привилегии один раз при входе (su) 2-Повышать привилегии каждый раз (sudo)

Прочие параметры задачи задаются аналогично.

Название задачи		Linux Audit
Цели сканирования	Группы активов	динамическая группа Linux (111)
Профиль		Unix Audit
Учетная запись First Login		Linux Auditor 1
Учетная запись Second Login		Linux Auditor 2

Когда эта задача завершится, можно будет изменить фильтр в группе Linux (111) на простой LinuxHost. В этом случае так же будет уместно переименовать ее из Linux (111) просто в Linux.

5. Создайте задачу «Fast Pentest Windows», указав в качестве цели динамические группы Windows и Linux (111) с профилем Fast PenTest (это системный профиль), и запустите ее.

Название задачи		Fast Pentest
Цели сканирования	Группы активов	Динамические группы Windows и Linux (111)
Профиль		Fast PenTest
Сканировать только отвечающие узлы		True

Группировка активов

Для управления активами в системе MaxPatrol SIEM используются статические и динамические группы активов. Статическая группа наполняется администратором вручную, динамическая наполняется автоматически на основании критерия, сформулированного на языке PDQL. Динамическая группа обязательно должна быть вложена в статическую. В интерфейсе системы можно сделать так, что группа будет отображать активы вошедшие во все вложенные подгруппы, таким образом, статическая группа тоже может наполняться автоматически, за счет вложенных в нее динамических групп.

Статические и динамические группы создаются при помощи меню, вызываемого кнопкой с тремя точками (см. Рисунок 2.6)

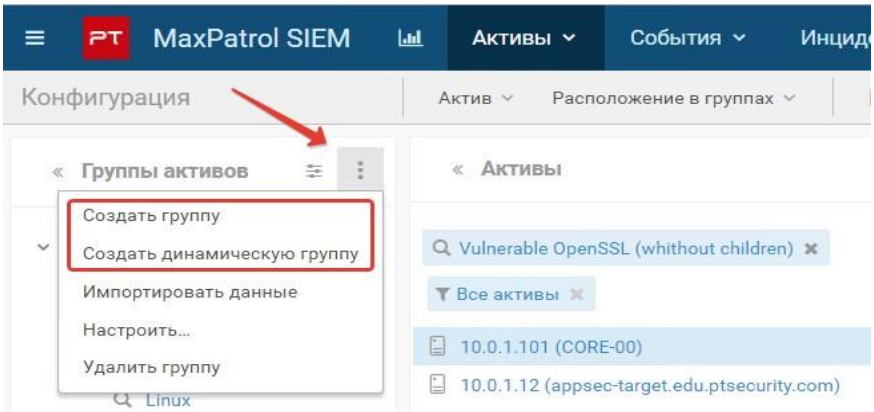


Рисунок 2.6 – Создание новой группы

Для создания запроса на языке PDQL в системе имеется специальный конструктор. Его возможности не исчерпывающи, но они позволяют сконтруировать запрос, не владея информацией о том, как устроена объектная модель актива в продукте. Запрос на языке PDQL может обращаться к любому атрибуту модели актива. Так как модель весьма сложна, без конструктора можно написать только самый простой запрос.

Динамические группы. Язык запросов PDQL

Для того, чтобы разобраться как обращаться к разным атрибутам модели актива, давайте посмотрим на примере как выглядят некоторые запросы. Далее мы будем пользоваться терминами объектно-ориентированного программирования «класс», «экземпляр», «атрибут». В корне иерархии

модели лежат классы Host и WebSite. Мы рассмотрим класс Host, от него унаследован класс Computer, а от него классы WindowsHost и LinuxHost (см Рисунок 7). Это значит, что если специалист хочет работать с атрибутом класса Host, то он должен сделать корневым объектом в запросе PDQL – Host, но если ему надо обратиться к атрибуту, который свойственен только классу WindowsHost, пользователь должен уточнить тип. Для этого в угловых скобках указывается интересующий наследника корневого класса.

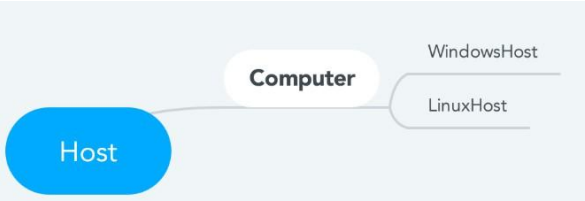


Рисунок 2.7 – Схема наследования классов от объекта Host (фрагмент)

Следующий запрос проверяет значение атрибута Fqdn класса Host:

Host.Fqdn = "core-00.edu.ptsecurity.com"

Чтобы обратиться к атрибуту класса, мы использовали оператор «точка». Fqdn это атрибут свойственный всем активам, унаследованным от класса Host, поэтому нам не понадобилось уточнять класс. А вот чтобы обратиться к атрибуту Workgroup, нужно обратиться к наследнику класса Host – классу WindowsHost:

Host<WindowsHost>.Workgroup = "Workgroup"

У класса Host нет атрибута Workgroup, поэтому мы уточнили наследника при помощи угловых скобок. Если у нас стоит задача просто найти все активы под управлением любой операционной системы семейства Windows, то мы можем просто указать класс, не обращаясь к его атрибутам. Достаточно написать:

Host<WindowsHost>

В части выражения PDQL до первой точки можно сократить запрос сразу обратившись напрямую к конечному наследнику. Такс следующие два запроса эквивалентны:

Host<WindowsHost> то же что просто WindowsHost

Другой пример. Посмотрим на Рисунок 8. У класса Host есть атрибут Softs (не Software!) этот атрибут может содержать в себе экземпляр класса Software или его наследника. Таким образом, чтобы найти актив, на котором установлен антивирус Касперского, можно использовать следующее выражение PDQL:

Host.Softs<KasperskyAntivirus>

На этот раз уточнение типа, т.е. указание конечного наследника в угловых скобках обязательно. Выражение Host.KasperskyAntivirus работать не будет, потому что у класса Host нет атрибута KasperskyAntiVirus.

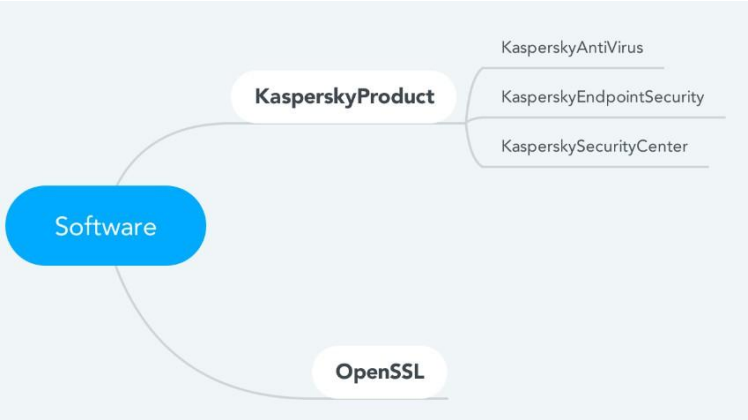


Рисунок 2.8 – Схема наследования классов от объекта Software (фрагмент)

Впрочем, возможно существование ПО, для которого в модели актива Positive Technologies не предусмотрено наличие отдельного класса – наследника Software. Поэтому наиболее универсальный способ найти актив на котором установлено некоторое ПО – проверить имя актива. Следующие два запроса найдут активы с установленным на них OpenSSL:

Host.Softs<OpenSSL>

и

Host.Softs.Name = "OpenSSL"

Для того, чтобы обратиться сразу к нескольким атрибутам модели актива, можно использовать конструкции с квадратными скобками. Следующий запрос находит активы с открытым портом 3389:

Host.Endpoints<TransportEndpoint>[Status = 'Open' and Protocol = 'tcp' and Port = 3389]

Тот же запрос можно переписать и так:

Host[Endpoints<TransportEndpoint>[Status = 'Open' and Protocol = 'tcp' and Port = 3389]]

Здесь идет обращение к атрибуту класса Host – Endpoints. В этом атрибуте располагается экземпляр класса Endpoint (названия почти совпали) или его наследника. Нам интересен его наследник TransportEndpoint. В свою очередь, у TransportEndpoint семь атрибутов, а с учетом атрибутов корневого класса Endpoint – все десять. Но нас интересуют три атрибута TransportEndpoint: Status (Open или Close), Protocol (tcp, udp или иной транспортный протокол) и Port (3389).

Для того, чтобы написать такое выражение надо хорошо представлять как устроена объектная модель актива. Однако модель настолько сложна, что документировать ее полностью затруднительно, как и пользоваться подоюной докуметацией. Поэтому в системе MaxPatrol SIEM реализован графический конструктор PDQL выражений. Он не полнофункционален в том смысле, что он не отображает все доступные в PDQL операторы, есть и другие ограничения, но конструктор позволяет решить главную задачу – навигацию по модели актива. Давайте при помощи конструктора составим выражение,

которое ищет все активы, которые получили DHCP аренду с «неправильного» DHCP-сервера.

Возьмем актив, подвергнутый аудиту, в правой части экрана выберем закладку «Конфигурация» и развернем признак «Интерфейсы/Local Area Connection 2/L3Settings/L3Settings». Кликнем по ссылке true атрибута DhcpEnabled (см. Рисунок 2.9).

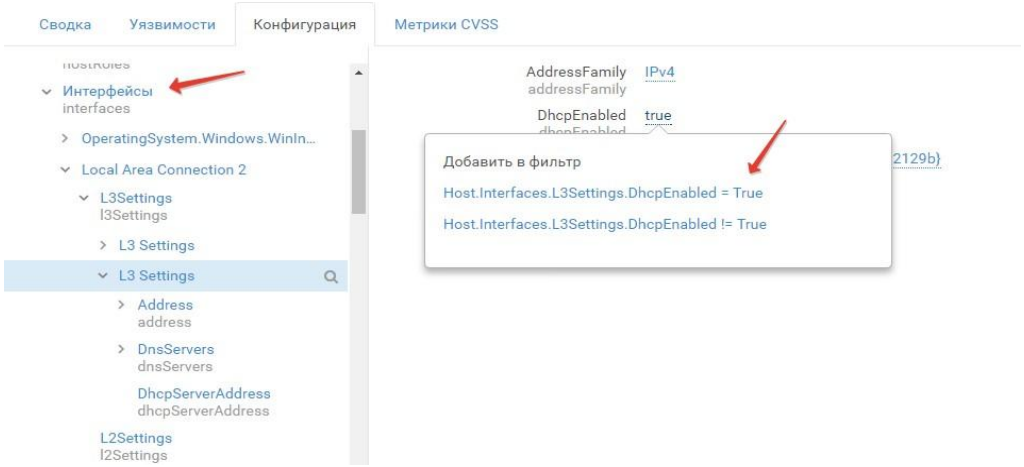


Рисунок 2.9 – Формирование PDQL-запроса при помощи конструктора

После клика у нас формируется выражение, которое находит все активы, у которых есть хотя бы один интерфейс получающий адрес по DHCP:

Host.Interfaces.L3Settings.DhcpEnabled = True

Здесь же найдем атрибут DhcpServerAddress и добавим его с отрицанием (см Рисунок 2.10).

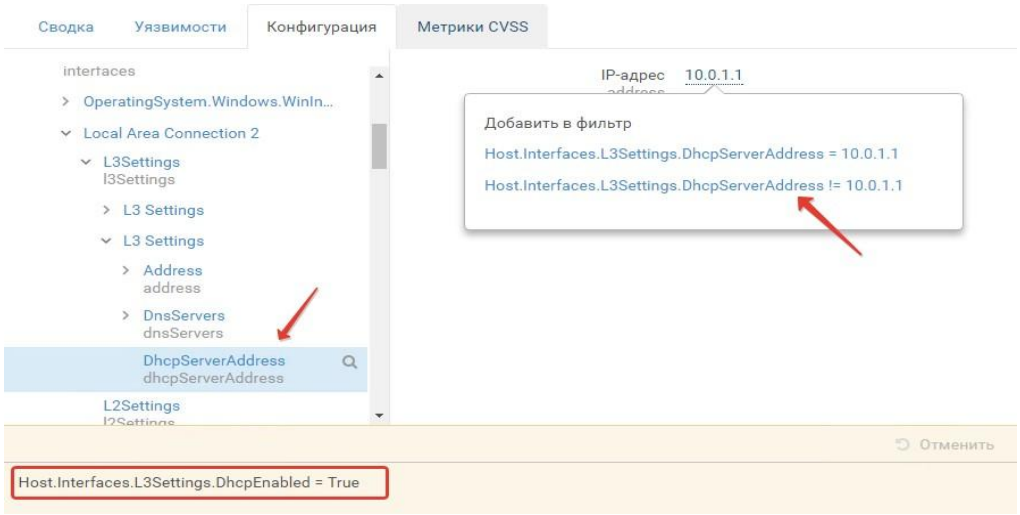


Рисунок 2.10 – Формирование PDQL-запроса при помощи конструктора

Таким образом, мы при помощи конструктора, сформировали выражение, которое ищет все активы, получившие аренду от сервера DHCP, чей адрес не равен доверенному 10.0.1.1:

Host.Interfaces.L3Settings[DhcpEnabled = True and DhcpServerAddress != 10.0.1.1]

Теперь конструктор позволяет поместить текущее выражение в буфер или перейти к созданию динамической группы с этим выражением (см Рисунок 11). При создании динамической группы у нас будет возможность отредактировать выражение.

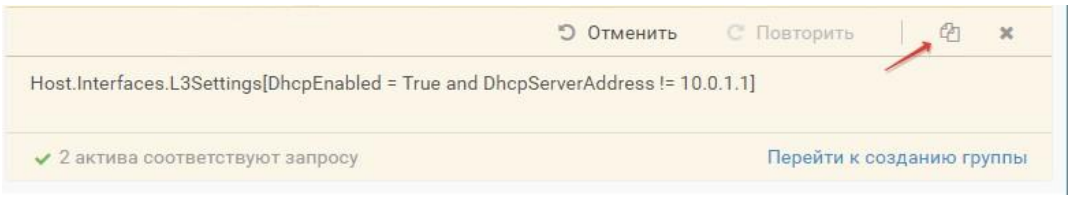


Рисунок 2.11 – Итог работы конструктора выражения PDQL. Стрелка указывает на кнопку копирования в буфер обмена

Теперь давайте обратимся к Рисунку 12. Если на предыдущих рисунках были показаны схемы наследования различных классов, то здесь показана схема атрибутов (встречающихся по тексту примеров). Заметьте, что в PDQL-выражении приводится именно название атрибута, а не название класса, экземпляр которого содержится в этом атрибуте (исключением является только TransportEndpoint, который понадобился для уточнения класса Endpoint находящегося в атрибуте Endpoints, вот почему TransportEndpoint взят в угловые скобки). Тот факт, что в выражении PDQL приводятся названия атрибутов, приводит к тому, что выражения иногда оказываются несовсем ясными. Для того, чтобы обратиться к IP-адресу присвоенному сетевому интерфейсу, приходится обращаться к атрибуту Host.Interfaces.L3Settings.Address.Address.Address. Но при этом в первом атрибуте Address располагается экземпляр класса InterfaceAddress (ведь настройки уровня L3 (L3Settings) могут быть разные, не только адрес), у которого тоже есть атрибут Address, в котором в свою очередь располагается экземпляр класса IPAddress (ведь адреса у интерфейса могут быть разные, не только IP), у которого тоже есть атрибут Address и вот он уже имеет представление, которое можно сравнивать со значением 192.0.2.123.

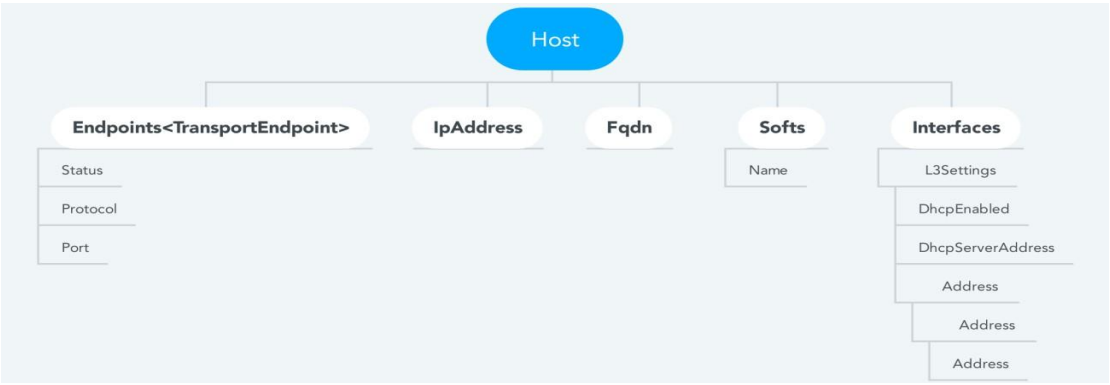


Рисунок 2.12 – Схема атрибутов класса Host (фрагмент)

Еще раз посмотрите на Рисунок 2.9. Вы видите, что адрес узла может располагаться не только в атрибуте Host.Interfaces.L3Settings.Address.Address.Address, но и в более коротком Host.IpAddress. Разница между этими атрибутами в том, что первый содержит адрес, назначенный реальному сетевому интерфейсу. Этот атрибут становится доступен только по результатам аудита (мы его еще не проводили). В то же время второй атрибут содержит

«видимый» адрес актива, по которому актив могут наблюдать модуль pentest или hostdiscovery. Этот адрес необязательно принадлежит данному активу. Реально это может оказаться пограничный DNAT-транслятор.

Мы видим, что IP-адреса могут по разным причинам располагаться в разных узлах дерева модели актива. Для того чтобы обратиться ко всем адресам актива, в каком бы месте модели они ни оказались можно воспользоваться алиасом @IP. Следующее выражение соберет в одну группу все узлы, которые возможно принадлежат сети 192.0.2.0/28:

Host.@IP in 192.0.2.0/28

«Возможно», потому что в данное выражение попадет и атрибут Host.IpAddress значение которого, как было сказано, не обязательно принадлежит узлу. Поэтому для создания динамической группы, содержащей все узлы из сети 192.0.2.0/28 правильнее использовать следующее выражение:

Host.Interfaces.L3Settings.Address.Address.Address in 192.0.2.0/28

Другой пример, где нужно использование алиасов иллюстрирует запросы к базе знаний PTKB относительно уязвимостей на узлах в информационной системе. Дело в том, что информация об уязвимостях не полностью располагается в модели актива. Уязвимость может быть привязана к конкретному порту и ПО, если она обнаружена модулем pentest. Но чаще мы узнаем об уязвимости из аудита. В этом случае аудит собирает информацию о версии программного обеспечения, а в базе знаний располагается информация о том, какие уязвимости свойственны данной версии. С одной стороны, это приводит к тому, что в модели нет информации о конкретной уязвимости, с другой стороны при обновлении базы знаний система получает информацию о новых уязвимостях активов без необходимости пересканировать их. Ввиду того, что информация об уязвимостях в модели отсутствует, доступ к ней из PDQL так же реализован через алиас @Vulners. Так, следующее выражение находит все активы с уязвимым OpenSSL:

Host.Softs<OpenSSL>.@Vulners

Следующее выражение делает то же самое, но не через явное задание наследника класса Software, а через атрибут Sots.Name:

Host.Softs[@Vulners and Name = "OpenSSL"]

Наконец, для создания группы активов с уязвимостью CVE-2017-0145 (через нее распространялся шифровальщик WannaCry) можно применить следующее выражение на PDQL:

Host.@Vulners.CVE = "CVE-2017-0145"

Фактически у любой ноды любого наследника класса Host или WebSite есть виртуальный атрибут @Vulners, У которого в свою очередь четыре

атрибута: Name, Description, CVE и PTKB (последние два это идентификаторы по базе CVE и PTKB соответственно).

Таблица 2.2 – Алиасы, псевдонимы в выражениях PDQL

Псевдоним	Область определения	Значение	
@Vulners	Любая нода любого наследника классов Host и WebSite	@Vulners.Name	Название уязвимости
		@Vulners.Description	Описание уязвимости
		@Vulners.CVE	'CVE-2017-0000'
		@Vulners.PTKB	Индекс PTKB
@IP	Host.@IP (или наследник Host)	Host.IpAddress Host.Interfaces.L3Settings.Address.Address.Address Host.Endpoints<IpEndpoint>.Address	
@MAC	Host.@MAC (или наследник Host)	Host.Interfaces.L2Settings.MacAddress Host.MacAddress Host.Endpoints<EthernetEndpoint>.Mac Host<Computer>.NetworkCard.Mac	
@Name	Host.@Name WebSite@Name	Поиск по DysplayName: имя паспорта актива или IP, FQDN	
@Description	Host.@Description WebSite@Description	Описание актива	

Снова посмотрим на выражение строящее группу узлов, чьи адреса принадлежат некоторой подсети. В этом выражении применялся оператор in. Конструктор выражений PDQL может использовать только операторы = и != (равно и не равно). Но синтаксис языка шире возможностей конструктора. Он включаеит и операторы сравнения и операторы членства в списке или в подсети, операторы like и match (см Таблица 2.3).

Таблица 2.3 – Операторы PDQL – языка запросов к модели активов

Оператор	**Синтаксис**	**Тип A**	**Тип B**	**Комментарий**
= !=	A = B A != B	строка		Сравнение без учета регистра
		целое число		
		IP-адрес		Сравниваются как числа, сравнение разных версий даст False
		*	null	
		булево значение		
		ДатаВремя		
> >= < <=	A > B A >= B A < B A <= B	строка		Сравнение без учета регистра, согласно лексикографическому порядку
		целое число		
		IP-адрес		Сравниваются как числа, сравнение разных версий даст False
		ДатаВремя		

Оператор	Синтаксис	Тип A	Тип B	Комментарий
in	A in B	строка	массив строк	Для каждого и элемента списка B_i выполняется регистронезависимое сравнение
		число	массив чисел	
		IP-адрес	сеть	Проверка вхождения адреса в сеть, указанную для адреса не того типа, дает False
		IP-адрес	массив адресов	
		IP-адрес	массив сетей	
Like	A like B	строка		B определяет шаблон, т.н. like-выражение (см. пояснение в тексте). Like-выражение работает регистронезависимо
Match	A match B	строка		B определяет шаблон регулярного выражения в стандарте POSIX. Оператор работает регистронезависимо
And	A and B	булево значение		Если предикаты A и B дают выборки, возвращается пересечение выборок
Or	A or B	булево значение		Если предикаты A и B дают выборки, возвращается объединение выборок
Not	not A not (A);	булев		
	A not in B A not like B A not match B	оператор		

В Таблица 2.3 приведены операторы языка PDQL. Как уже было сказано, при помощи конструктора можно добавить только операторы = и !=, но вручную при редактировании группы можно использовать любой из приведенных операторов.

Выражения Like широко распространены в различных базах данных и являются частью синтаксиса SQL. Выражения Like фактически являются шаблонами Wildcard. В них применяется два оператора:

% – любое количество любых символов и _ (подчерк) – любой символ. Шаблоны Match более функциональны, и позволяют использовать регулярные выражения в стандарте POSIX.

Так же остановимся на некоторых тонкостях применения оператора not. Следующее выражение ищет все активы, у которых есть хотя бы одно ПО, но ни одно из ни них не называется OpenSSL:

Host.Softs.Name not like "OpenSSL"

А вот это выражение делает то же самое, но ему так же соответствуют активы, у которых вообще нет никакого ПО:

not Host.Softs.Name like "OpenSSL"

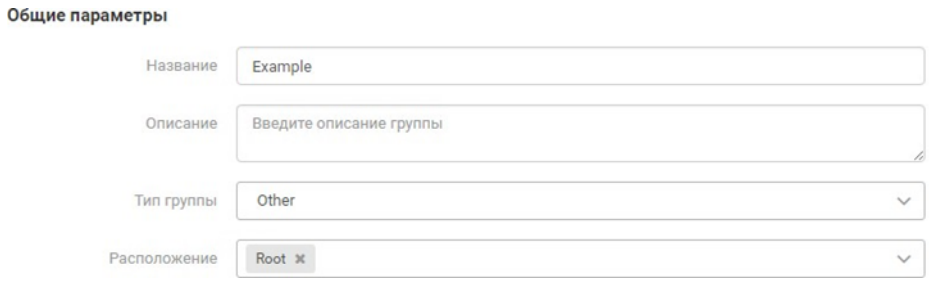
Фактически оператор not поставленный перед объектом модели последовательно применяется ко всем атрибутам. Так, следующий оператор ищет все активы у которые:

- вообще не являются Windows-хостами или наследниками WindowsHost (наследников вообще-то нет, но все же),
- Windows-хосты, на которых нет никакого ПО,
- Windows-хосты, на которых какое-то ПО есть, но это не OpenSSL:

not WindowsHost.Softs.Name = "OpenSSL"

Таблица 2.4 – Некоторые примеры PDQL запросов к модели активов

Найти определенное ПО	Host.Softs<TeamViewer>
Сделать группу с серверами Apache, чтобы потом использовать ее как цель для сбора журналов	UnixHost.Softs.Name like '%Apache%'
Найти узлы с некоторой уязвимостью	Host.@Vulners.CVE = 'CVE-2017-0000'
Рабочие станции без антивируса Касперского	WindowsHost and not WindowsHost.Softs<KasperskyAntiVirus>
Узлы Cisco IOS с неудачными настройками журналирования	IOSHost.Services<IOSLogging>[ConsoleSeverityLevel = 'debug']
Найти все узлы с RDP, чтобы просканировать их пентестом на предмет наличия определенной уязвимости	WindowsHost.Endpoints<TransportEndpoint>[Status = 'Open' and Protocol = 'tcp' and Port = 3389]
Найти все не Windows-узлы, чтобы просканировать их по ssh	not WindowsHost
Решение задачи инвентаризации: найти все активы, подключенные одним из активных интерфейсов в подсеть	Host.Interfaces[Status = 'Up' and L3Settings.Address.Address.Address in 192.0.2.0/28]
Найти все активы, не подключенные в подсеть	not Host.Interfaces[Status = 'Up' and L3Settings.Address.Address.Address in 192.0.2.0/28]
Найти узлы из сети 192.0.2.0/24 с операционной системой Cisco ASA и уязвимостью CVE-2017-0000	Host[OsName like '%ASA%' and Interfaces[Status = 'Up' and L3Settings.Address.Address.Address in 192.0.2.0/24] and @Vulners.CVE = 'CVE-2017-0000']
Выявить клиентов получивших аренду от нелигитимного DHCP-сервера, где легитимные 192.0.2.5 и 192.0.2.6	Host[OsName like '%Windows%' and Interfaces[Status = 'Up' and L3Settings[DhcpEnabled = true and DhcpServerAddress not in [192.0.2.5,192.0.2.6] and Address.Address.Address in 192.0.2.0/24]]]
Узел с двумя разными браузерами конкретных версий	Host.Softs[Name like '%Chrome%' and Version = '52'] and Host.Softs[Name like '%Firefox%' and Version = '15']
Веб-сайты, зараженные шеллкодом	Website.Pages.Path = '/wsoshell.php'
Ищем уязвимость по имени и описанию	Host.@Vulners[Description like '%someDesc%' and Name like '%someName%']
Ищем узлы с уязвимым антивирусом Касперского	WindowsHost.Softs<KasperskyAntiVirus>.@Vulners
Рабочие станции директоров	Host.@Description like '%дирекция%'



Из последующего задания фильтра, определяющего критерии группировки активов.

В качестве примеров можно представить следующие фильтры:

Фильтр	Критерий
Host.@Vulners.CVE="CVE-2017-0145"	Все активы с обнаруженной CVE-2017-0145
Host.Interfaces.L3Settings[DhcpEnabled = True and DhcpServerAddress != 10.0.1.1]	Все активы с IP адресом полученным от неверного DHCP
Host.Interfaces.L3Settings.Address.Address.Address in 10.0.1.0/26	Все активы входящие в сегмент сети 10.0.1.0/26
Host.Endpoints<TransportEndpoint>[Status = 'Open' and Protocol = 'tcp' and Port = 3389]	Активы с открытым портом 3389 транспорта TCP
Host.Softs[@Vulners and Name = "OpenSSL"]	Активы с открытым SSL
Host.Softs<OpenSSL>.@Vulners	

Особое внимание стоит обратить на возможности написания фильтров. SIEM имеет удобный конструктор для составления фильтров, работающий по принципу включения или исключения заданных критериев, однако возможности фильтров не ограничиваются конструктором. К примеру, конструктор не умеет обращаться у дочерним веткам параметров активов, записываемых в угловых скобках. Такого вида фильтр составляется в ручном режиме.

Задание 1

Ознакомление с дополнительными кейсами при создании динамических групп. Научиться составлять на языке PDQL запросы к базе активов.

Рекомендуется ознакомиться с разделом «Динамические группы. Язык запросов PDQL». Создайте в группе Example следующие динамические группы:

Название группы	Какие активы должны попасть в группу
10.0.1.0/26	Активы, у которых есть интерфейс с адресом из сети 10.0.1.0/26
WannaCry Vulnerable	Активы с уязвимостью CVE-2017-0145
Vulnerable OpenSSL	Активы на которых установлен уязвимый OpenSSL
Wrong DHCP	Активы, получившие аренду с DHCP сервера, чей адрес отличается от 10.0.1.0/24

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

Отчет должен включать:

– титульный лист;

– цель работы;

– ход работы, содержащий пошаговое описание осуществленных действий, иллюстрированных скриншотами на каждом этапе выполнения;

– вывод.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Практическая работа № 3

Тема. Концептуальные положения организационного обеспечения информационной безопасности

Цель занятия: Ознакомление с контекстными метриками CVSS и понятием «Важность актива» (Asset Importance).

Теоретическая часть:

Архитектура и системные требования

MaxPatrol SIEM – многокомпонентный продукт, который состоит из следующих частей:

• Core – осуществляет централизованное управление всеми компонентами системы и хранение конфигурации активов – данных о компьютерах и устройствах в сети. Здесь же реализовано управление системой через веб-интерфейс.

• SIEM – осуществляет обработку событий: агрегацию, нормализацию и корреляцию. Хранение событий может осуществляться на компоненте SIEM, но может быть и вынесено на отдельный узел (или кластер) для высоконагруженных систем (подробности см. в Administrator Guide). Так же SIEM может быть установлен на Agent (см. ниже) для распределения работ по аггрегации и нормализации (но не корреляции) данных.

• Agent – многомодульная платформа для сканирования сети и сбора событий.

• PTKB – база знаний. Обычно устанавливается вместе с ядром (Core), но может быть установлена отдельно. Ее назначение состоит в том, чтобы предоставить клиенту или партнеру интерфейс для работы с правилами нормализации и корреляции. В работе системы не принимает участия. Ядро использует для работы свою реплику PTKB. Но именно через PTKB осуществляется получение новых правил от компании Positive Technologies.

• UCS – Update and Configuration Server. Компонент предназначен для сетевого обновления других компонен системы. В работе системы участия не принимает.

Системные требования компонентов MaxPatrol SIEM напрямую зависят от требуемой производительности (количество событий в секунду – EPS) и

времени хранения их в системе. Схемы развертывания подробно обсуждаются в документе Administrator Guide.

Компоненты поддерживают работу в следующих операционных системах:

- Core, SIEM, Agent, PTKB – Microsoft Windows Server 2008 R2 SP1 или Microsoft Windows Server 2012/2012 R2;
- SIEM, PTKB, UCS – GNU/Linux Debian 8.6.

Для доступа к компонентам системы рекомендуется использовать браузеры Google Chrome 49 (и выше), Mozilla Firefox 45 (и выше) или Internet Explorer 11 (и выше).

Схема учебного стенда MaxPatrol SIEM

Схема учебного стенда MaxPatrol SIEM приведена на рисунке 3.1.

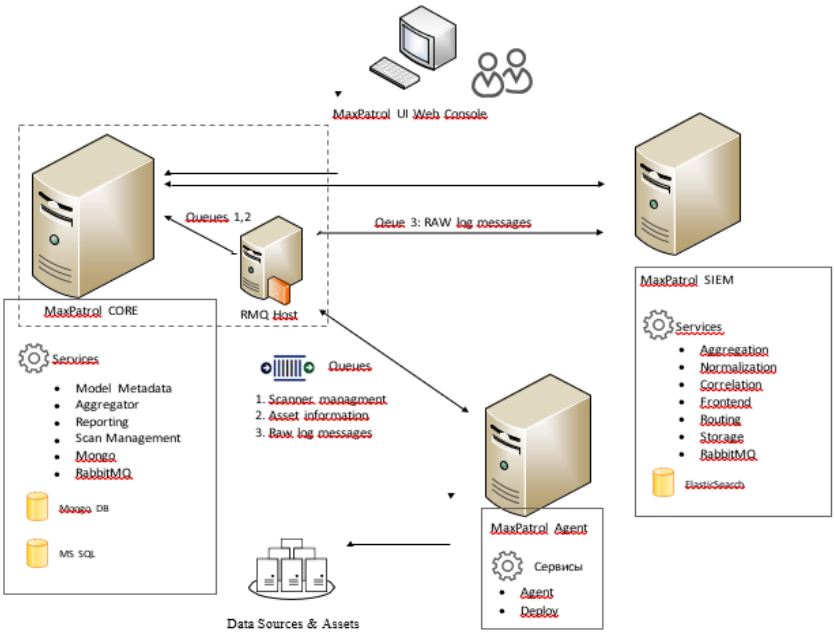


Рисунок 3.1 – Схема учебного стенда MaxPatrol SIEM

Задания по практическим занятиям посвящены работе с системой MaxPatrol SIEM. Одна из задач учебного курса состоит в подготовке к работе оператора системы.

В рамках настоящего курса студенты будут работать на учебных стендах в минимально возможной конфигурации – standalone. Все компоненты системы устанавливаются на один компьютер под управлением ОС Windows Server 2008 R2.

Методические рекомендации по выполнению практического занятия

1. Перейдите в группу Windows и выберите один из Windows-активов. На вкладке Сводка запомните значение интегральной уязвимости узла. Обратите внимание на шкалу времени. Необходимо, чтобы она отображала состояние актива «на сейчас».

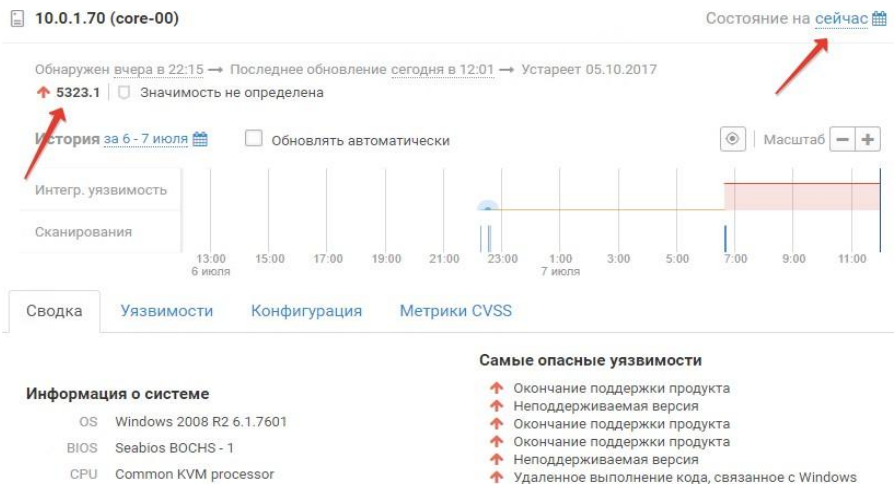


Рисунок 3.2 – Состояние актива

2. Нажмите кнопку «Актив/Редактировать паспорт» и установите Требования к конфиденциальности узла «Низкая». Интегральная уязвимость узла снизится, так как будет автоматически пересчитаны значения уязвимостей, наносящих ущерб конфинециальности узла. Так же автоматически будет определена значимость узла как низкая (значимость узла автоматически расчитывается из эффективных значений конфидециальности, целостности и доступности).

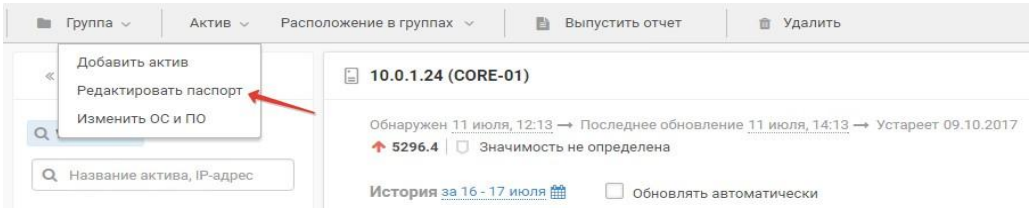


Рисунок 3.3 – Редактировать паспорт

3. Отредактируйте группу активов Windows (меню Группа/Настроить…) и установите у группы требования к конфиденциальности активов Высокая.

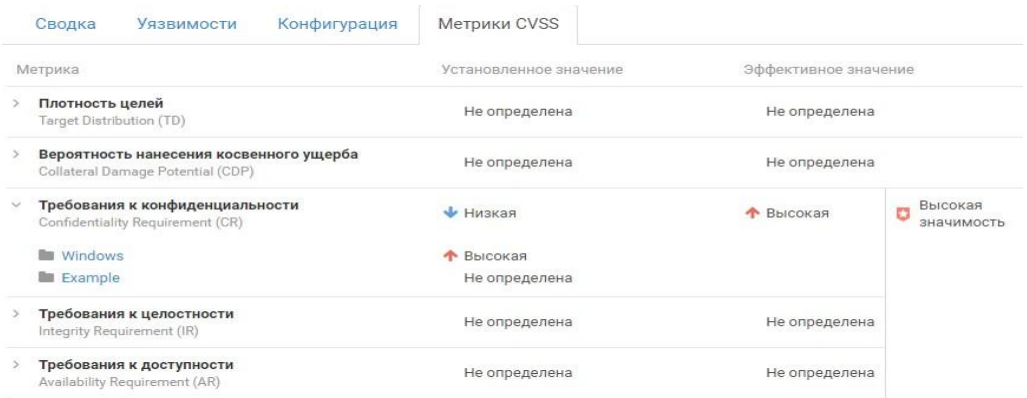


Рисунок 3.4 – Требования к конфиденциальности активов

Обратите внимание, хотя у выбранного актива установлено значение метрики Требования к конфидециальности Низкая, эффективное значение

метрики Высокая, т.к. актив входит в группу с такой метрикой. Значимость актива становится высокой, и интегральная уязвимость увеличивается.

Часть 5. Топология

Цель:

Научиться загружать ранее сделанные сканы в систему. Научиться работе с топологией сети.

1. На машине Core перейдите в консоль, из архива ScanData.0.50.4228-topology.nupkg извлеките папку audit (воспользуйтесь программой 7-Zip).
2. Распакованные XML-файлы поместите напрямую в Модель активов MPX-SIEM при помощи сервисной программы mp9cmd.exe:

C:\Users\Administrator>"c:\Program Files\Positive Technologies\MaxPatrol SIEM Core\MP9Cmd.exe" manualscan -i Downloads\audit

3. Новые активы, которые не соответствуют ни одному ранее сформированному критерию, попадут в группу Unmanaged hosts. Выделите группу «Все активы» и нажмите кнопку «Топология» в правом верхнем углу окна браузера.

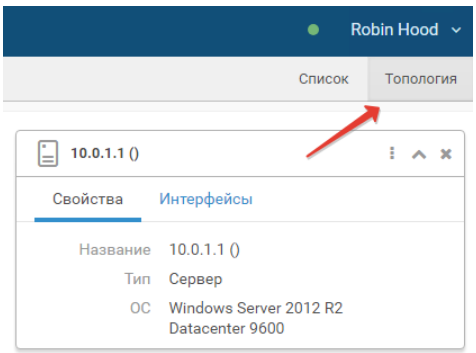


Рисунок 3.5 – Кнопка «Топология»

Внимание! Узлы не отобразятся в системе сразу по завершении работы описанной команды. Нужно время для того, чтобы обработать пришедшие данные. Вы можете запустить на машине Core диспетчер задач (команда taskmgr) и убедиться в том, что процесс PT.MaxPatrol.Assets.Processing.Host.exe работает и потребляет ресурсы.

4. Выберите на схеме межсетевой экран (иконка с символом кирпичной стены), в появившемся окне с карточкой актива изучите закладки «Свойства» и «Интерфейсы».

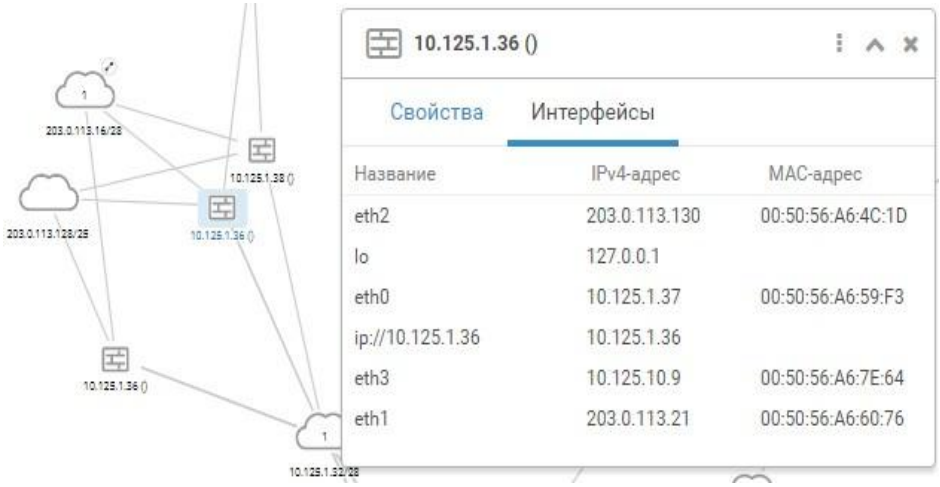


Рисунок 3.6 – Закладки «Свойства» и «Интерфейсы»

5. Выберете указателем иконку подсети (облачко на схеме). В закладке Активы отобразится перечень узлов из этой сети, маршрутизаторов, межсетевых экранов. Обратите внимание, что все адреса на диаграмме – это гиперссылки.

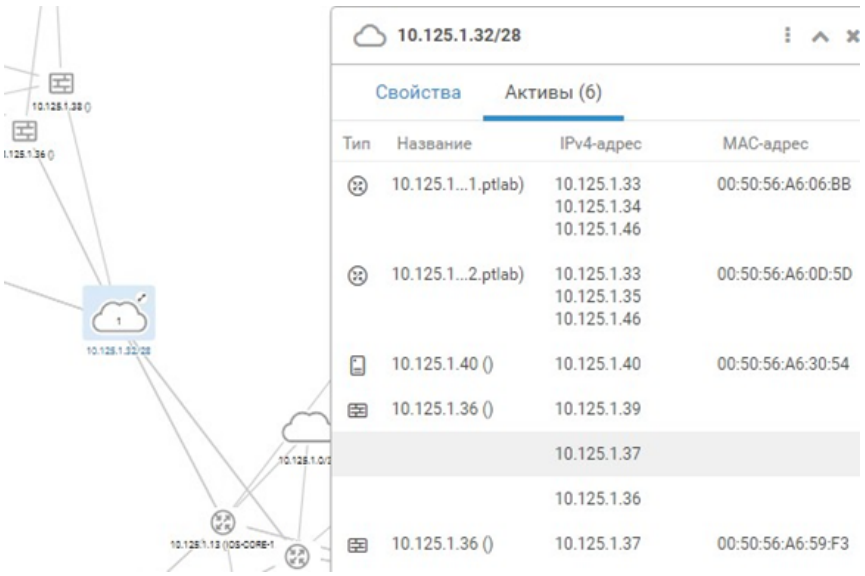


Рисунок 3.7 – Закладки «Свойства» и «Активы»

6. Заметьте два адреса на противоположных концах схемы. Кликните по одному из активов и в карточке актива вызовите меню (кнопка с тремя вертикальными точками). Выберите пункт меню «Куда открыт доступ».

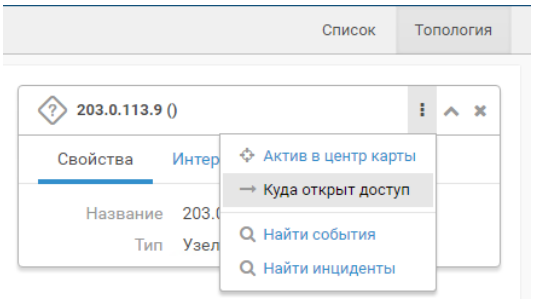


Рисунок 3.8 – Пункт меню «Куда открыт доступ»

7. В разделе «Цели» введите второй IP-адрес. При желании уточните протоколы и порты цели, затем нажмите кнопку «Рассчитать маршруты». Разверните список вычисленных маршрутов.

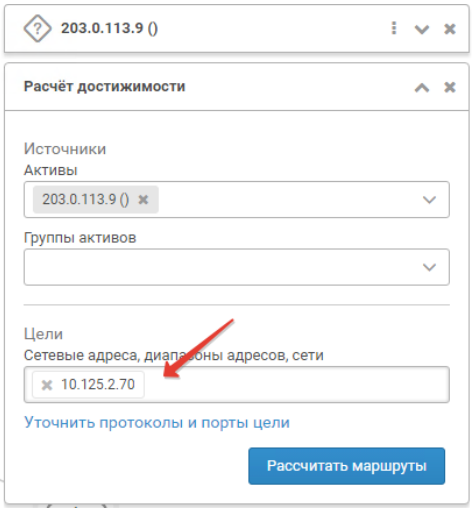


Рисунок 3.9 – Раздел «Цели»

8. На схеме отобразится один из маршрутов. Вы можете переключиться на другой маршрут, а также просматривать те фрагменты таблицы маршрутизации на промежуточных узлах, которые ответственны за реализацию данного пути.

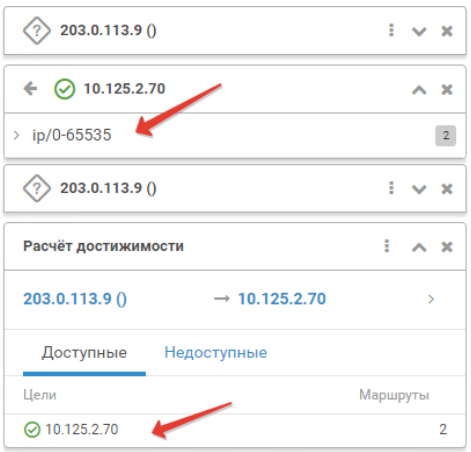


Рисунок 3.10 – Один из маршрутов

9. На приведенном рисунке 3.11 показано как переключаться между маршрутами и как просмотреть фрагмент таблицы маршрутизации на промежуточном узле. Виден статический маршрут до сети 10.125.0.0 через шлюз 10.125.1.49.

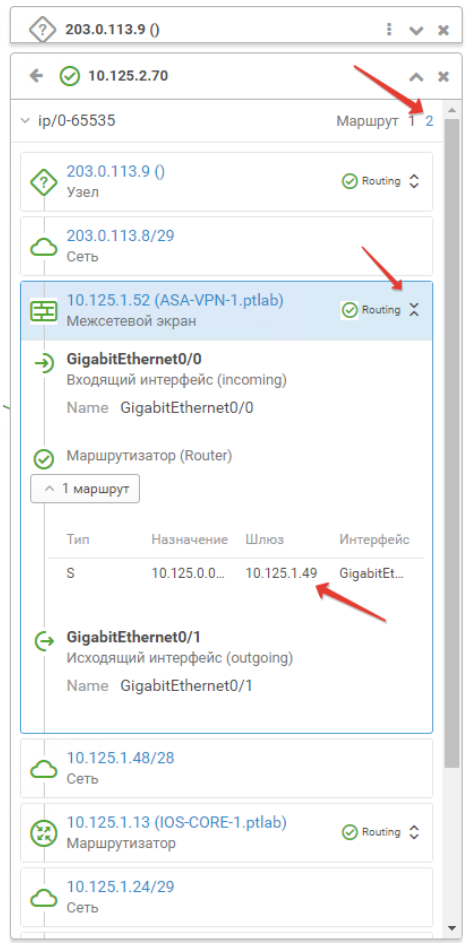


Рисунок 3.11 – Переключение между маршрутами

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

Отчет должен включать:

– титульный лист;

– цель работы;

– ход работы, содержащий пошаговое описание осуществленных действий, иллюстрированных скриншотами на каждом этапе выполнения;

– вывод.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Практическая работа № 4

Тема. Организация службы безопасности объекта

Цель занятия: Научиться создавать локальных и доменных пользователей в системе. Научиться назначать пользователям роли.

Теоретическая часть:

Агент Agent, Endpoint Monitor, Network Monitor

Функция агента состоит в сборе событий с источников данных и в проведении сканирований информационной системы. Собранные события агент оборачивает в JSON-конверт, добавляя к нему несколько служебных полей, в частности время получения события агентом. Начиная с релиза 14.0 появилась возможность на агенте выполнять также нормализацию и агрегацию данных (так называемый SIEM на агенте). Агент порождает потоки данных, которые очередями передаются на шину данных RabbitMQ (RMQ Host).

Сбор данных об информационных активах может осуществляться как посредством запуска различных задач типа PenTest, так и при помощи аудита с применением протоколов удаленного доступа (SSH/Telnet для Unix-подобных систем и сетевого оборудования или WMI для узлов под управлением ОС Windows).

Сбор событий также может осуществляться разными способами:

1. Агент может открыть на прослушивание порт 514, на который источники событий будут направлять события по протоколу syslog.
2. Агент может подключаться к источникам при помощи протоколов удаленного доступа и читать данные из файлов или использовать внутренние API для чтения журналов.
3. Также агент может использовать иные механизмы подключения к источникам: ODBC, OPSEC.

Источником данных для системы MaxPatrol SIEM может быть не только агент. Так, для операционной системы Windows выпущен модуль, который называется Endpoint Monitor. Его функция состоит в том, чтобы контролировать системную активность узла на уровне ядра. (следить за сетевой активностью узла, отслеживать обращения к файлам). Собранную информацию Endpoint Monitor направляет на шину данных, как и агент. Другим источником данных может выступать компонент Network Monitor (компонент устанавливается на Linux Debian), назначение которого – собирать информацию о сетевой активности.

Методические рекомендации по выполнению практического занятия

1. Нажмите кнопку меню с иконкой в виде трех горизонтальных полос в левом верхнем углу браузера и выберите пункт меню Identity and Access Managment.

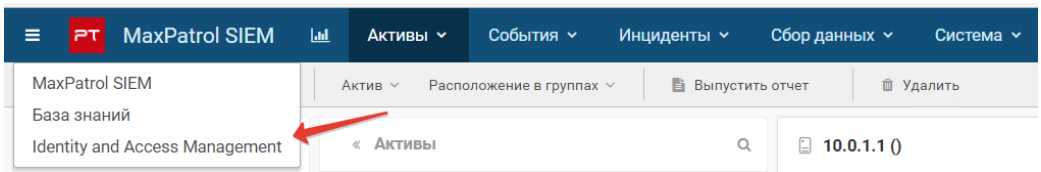


Рисунок 4.1 – Пункт меню Identity and Access Managment.

В разделе Identity and Access Management и MaxPatrol SIEM вы можете создавать, удалять, блокировать пользователей, менять им пароли, назначать

различные роли в различных системах, указывать электронную почту, а также контролировать их действия в системе. Обратите внимание, что, работая с сайтом PT IAM, вы работаете с системой не по порту 443, а по альтернативному порту 3334.

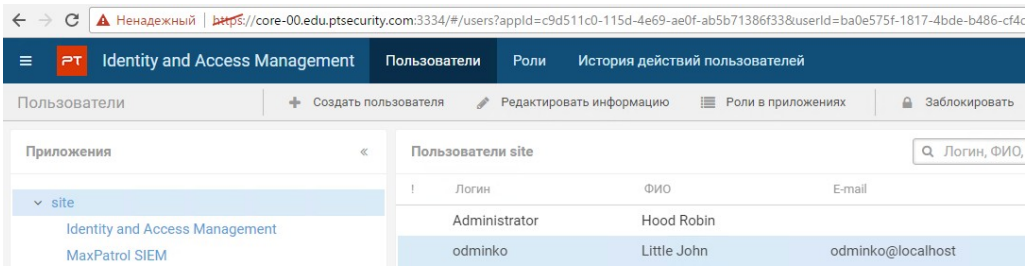


Рисунок 4.2 – Альтернативный порт

2. Для встроенной учетной записи Administrator назначьте имя и фамилию, например фамилия – Hood, имя – Robin. Для этого нажмите кнопку «Редактировать информацию».

3. Создайте пользователя odminko, для которого укажите фамилию/имя Little John, e-mail odminko@localhost.

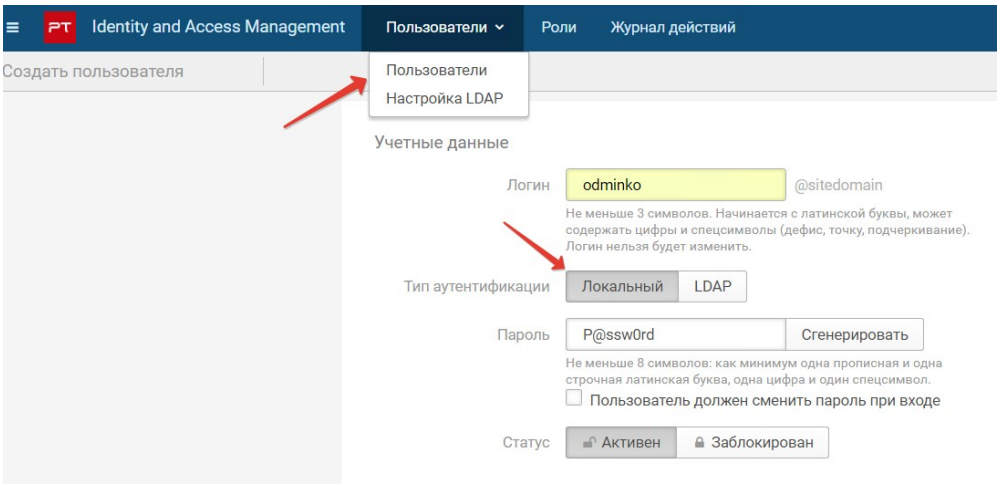


Рисунок 4.3 – Создание пользователя

4. Отмотайте диалог создания пользователя в самый низ. Сперва (в самом верху) вы увидите группу параметров «Учетные данные», потом «Персональные данные» (там вы задавали ФИО и email), потом «Организационная информация» и, наконец, «Назначить роли в приложениях». Назначьте пользователю роль Оператор в MaxPatrol SIEM и Operator в PT Knowledge Base.

Учетные данные	Логин	odminko
	Тип аутентификации	Локальный
	Пароль	P@ssw0rd
Персональные данные	Фамилия	Little
	Имя	John
	E-mail	odminko@localhost

Назначить роли в приложениях	Identity and Access Managment	Пользователь
	MaxPatrol Siem	Оператор
	PT Knowledge Base	Operator

Локальные пользователи создаются системой непосредственно в ядре MaxPatrol в базе данных PostgreeSQL. Удалить созданного пользователя или переименовать – нельзя. Это ограничение связано с тем, что действия пользователей журналируются. Пароль пользователя так же хранится в базе PostgreeSQL и требований парольной политики к нему не предъявляется. Если возникает необходимость предъявить требования к сложности пароля и к времени его устревания, то эта задача решается путем введения аутентификации через LDAP во внешней системе, например в Active Directory. Для создания учетной записи LDAP сперва нам надо сконфигурировать пул LDAP- серверов:

5. На вкладке «Пользователи/настройки LDAP» создайте новый пул серверов.

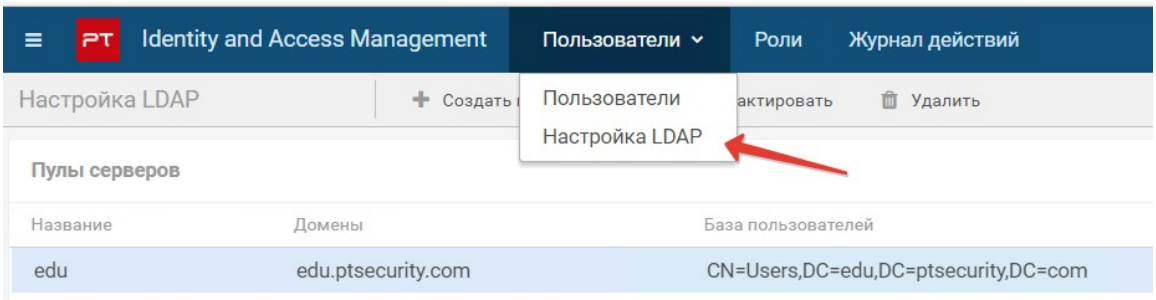


Рисунок 4.4 – Настройка пула

6. Назовите пул edu, укажите домен edu.ptsecurity.com. В поле «База пользователей» укажите ветвь дерева LDAP в которой расположены пользователи системы: CN=Users,DC=edu,DC=ptsecurity,DC=com

7. Укажите сервер 10.0.1.1 и снимите галочку с опции SSL (порт должен стать 389).

Название		edu
Домены		edu.ptsecurity.com
База пользователей		CN=Users,DC=edu,DC=ptsecurity,DC=com
Серверы	Адрес	10.0.1.1
	Порт	389 (не исправляйте, он сам таким станет)
	SSL	отключить

8. Дополнительно (не обязательно) можно проверить соединение с сервером LDAP. Для этого нажмите кнопку «Проверить соединение» (слева снизу) и введите логин (в формате prantagenet@edu.ptsecurity.com) и пароль. После подключения вы должны увидеть загруженные с сервера данные, в частности ваше ФИО.

Теперь надо создать пользователя, который будет аутентифицироваться по LDAP

9. Аналогично тому, как вы создавали пользователя odminko, создайте нового пользователя (себя) в системе.

Учетные данные	Логин	PositiveStudent
	Тип аутентификации	LDAP
	Доменное имя пользователя	plantagenet (введите свой логин для прохода к серверу учебных стендов)
	Алиасы	Выберите пул edu, поле заполнится автоматически
	Получать персональную иорганизационную информацию с сервера	включить
Назначить роли в приложениях	Identity and Access Managment	Администратор
	MaxPatrol Siem	Администратор
	PT Knowledge Base	Admin

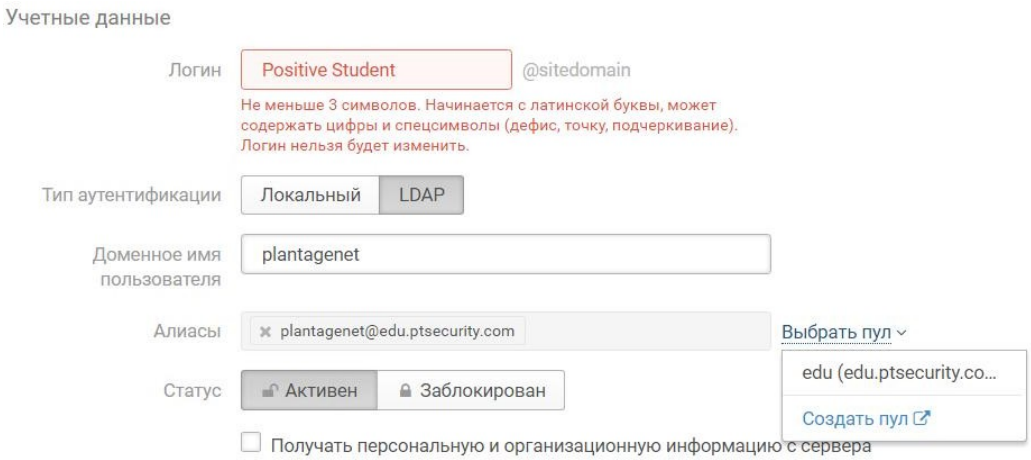


Рисунок 4.5 – Пользователь PositiveStudent

Информация о том, как вас зовут и какая у вас почта (если она есть) будет подгружена с сервера LDAP автоматически и первом входе в систему.

10. Войдите в систему от своего имени. Для этого откройте новое окно браузера в режиме инкогнито, в окне входа в систему переключитесь на LDAP, укажите свой логин вместе с UPN-суффиксом (вида plantagenet@edu.ptsecurity.com) и пароль, который вы используете для входа в систему.

11. Снова переключитесь на список пользователей в незакрытом основном окне браузера и обновите страницу. Вы должны увидеть подгруженные из Active Directory ФИО.

12. Выберите закладку «Роли» и посмотрите, какие роли в каких системах есть, какие полномочия в них доступны.

13. Самостоятельно изучите возможности системы по регистрации действий пользователей на вкладке «История действий пользователей».

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

Отчет должен включать:

– титульный лист;

– цель работы;

– ход работы, содержащий пошаговое описание осуществленных действий, иллюстрированных скриншотами на каждом этапе выполнения;

– вывод.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Практическая работа № 5

Тема. Структура и деятельность службы безопасности

Цель занятия: Научиться выполнять сбор событий различных источников.

Теоретическая часть:

Функции Core, RMQ Host

Функции Core (ядро системы) и RQM Host чаще всего выполняются на одном узле, но на практике они могут быть и разнесены. Шина данных, в которую отправляются сообщения от агента, работает на основе системы Rabbit MQ (RMQ Host). Различные системные службы осуществляют подписку на очереди в RabbitMQ. При этом на очередь с сырыми событиями подписан сервис компонента SIEM и сырые события попадают в его шину данных.

В задачи ядра входят:

1. Сбор, обработка и хранение информации об информационной системе. Предоставление этой информации различным службам системы (для Siem ядро известно как AssetResolverHost).
2. Предоставление пользователю интерфейса (UI функционирует на основе веб-сервера MS IIS). Для отображения информации в UI ядро осуществляет как сбор данных с модели активов, так и выгрузку событий из Siem.
3. Построение отчетов.

Кроме того, веб-сервер IIS, установленный на Core, может обслуживать и иные компоненты платформы MaxPatrol 10, например PT IAM (Identity and Access Managment) на портах 3333/3334.

Данные, об активах из очереди в RabbitMQ попадают в реляционную базу PostgreeSQL.

Методические рекомендации по выполнению практического занятия

Часть 1. WinEventLog, WMInotification

1. Создайте задачу по сбору мониторинговой информации с Windows.

Название задачи		RAM Monitoring (Windows)
Цели сканирования	Группы активов	динамическая группа Windows
Профиль		Monitoring Windows RAM Load
Учетная запись		Windows Auditor

2. Создайте задачу по сбору событий с Windows.

Название задачи		Get Windows Event Logs
Цели сканирования	Группы активов	динамическая группа Windows
Профиль		WinEventLog
Учетная запись		Windows Auditor

Сохраните и запустите задачу. Задача будет все время в статусе running, так как по мере необходимости она будет все время подгружать новые события.

3. Создайте задачу по сбору мониторинговой информации с Linux (мониторинг осуществляется при помощи команды vmstat -s, повышенных привилегий она не требует).

Название задачи		RAM Monitoring (Linux)
Цели сканирования	Группы активов	динамическая группа Linux
Профиль		Monitoring Linux RAM Load
Учетная запись First Login		Linux Auditor 1
Учетная запись Second Login		–

 Возможности системы MaxPatrol SIEM позволяют осуществлять фильтрацию событий на разных стадиях их жизненного цикла. В профиле для сбора данных WinEventLog мы можем увидеть следующие строки (о том, как просмотреть и отредактировать профиль будет сказано ниже):

```
"log_channels": [
{
"file": "Security",
"query": "*"
},
{
"file": "Application", "query": "*"
},
{
"file": "System",
"query": "*"
},
{
"file": "Microsoft-Windows-NetworkProfile/Operational", "query": "*"
```

```
},
{
"file": "Microsoft-Windows-Dhcp-Client/Admin", "query": "*"
},
{
"file": "Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational", "query": "*"
},
{
"file": "Microsoft-Windows-Windows Firewall With Advanced Security/Firewall", "query": "*"
}
]
```

Из приведенного фрагмента можно видеть, что мы собираем данные из некоторых каналов, сообразно запросам, котрые формулируются на языке XPath (по умолчанию везде *, т.е. мы не фильтруем поток события на источнике). Фильтрация на источнике может понадобиться для снижения объема данных которые загружают канал передачи данных между источником и Агентом и далее по цепочке, для снижения объема данных, хранящихся в базе Elastic Search, причем как в индексе нормализованных событий, так и в индексе сырых событий, а так же для снижения нагрузки на вычислительные ресурсы SIEM'а. Частично можно добиться аналогичного эффекта установив SIEM на агент, однако для снижения нагрузки на канал между источником и Агентом данный прием безальтернативен.

События в системе Microsoft Windows Event Log хранятся в формате XML, чтобы увидеть его надо в программе EventViewer сделать двойной щелчок на событии и просмотреть вкладку «Подробности», переключив режим просмотра в XML:

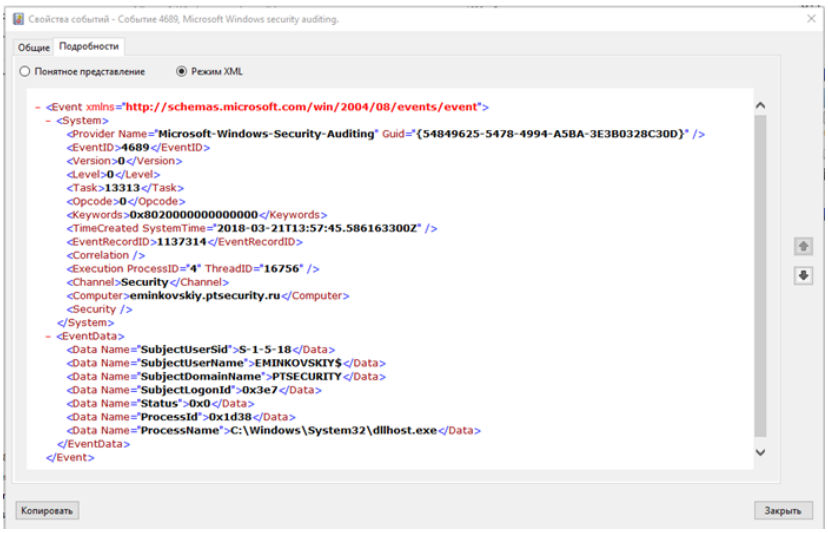


Рисунок 5.1 – Вкладка «Подробности»

Теперь для того, чтобы в канал отправились нужные нам данные, надо написать выражение на языке XPath описывающие ту или унную XML. За

информацией о том, как это делать можно обратиться к справке системы Microsoft, мы же покажем здесь некоторые примеры выражений:

Следующий запрос приводит к тому, что события с EventID из перечисленного списка не попадут на Агент. Внимание! Перечисленные 23 события взяты наугад, их список ни в каком виде не является рекомендацией Positive Technologies.

*[System [(EventID!=4624 and EventID!=4776 and EventID!=4770 and EventID!=4625 and EventID!=4648 and EventID!=4932 and EventID!=4933 and EventID!=4670 and EventID!=4907 and EventID!=4742 and EventID!=4740 and EventID!=4662 and EventID!=4723 and EventID!=4738 and EventID!=5059 and EventID!=5447 and EventID!=4611 and EventID!=4931 and EventID!=4688 and EventID!=5058 and EventID!=4622 and EventID!=4724 and EventID!=4614)]]

Следующий запрос белый список, т.е. наоборот, только события из указанного перечня попадут на Агент:

*[System [(EventID=4624 or EventID=4776 or EventID=4770 or EventID=4625 or EventID=4648 or EventID=4932 or EventID=4933 or EventID=4670 or EventID=4907 or EventID=4742 or EventID=4740 or EventID=4662 or EventID=4723 or EventID=4738 or EventID=5059 or EventID=5447 or EventID=4611 or EventID=4931 or EventID=4688 or EventID=5058 or EventID=4622 or EventID=4724 or EventID=4614)]]

Опыт показывает, что больше 23 альтернатив в выражении XPath будет отвергнуто Windows, это опытная величина. Positive Technologies не может ручаться что так будет всегда и везде. Поэтому, прежде чем сделать данную настройку в профиле MaxPatrol SIEM, попробуйте применить данный фильтр в Event Viewer. В панели справа от списка событий нажмите по кнопке «Фильтр текущего журнала», перейдите на вкладку XML, выберите чекбокс «Изменить запрос вручную» и вместо звездочки впишите проверяемый запрос:

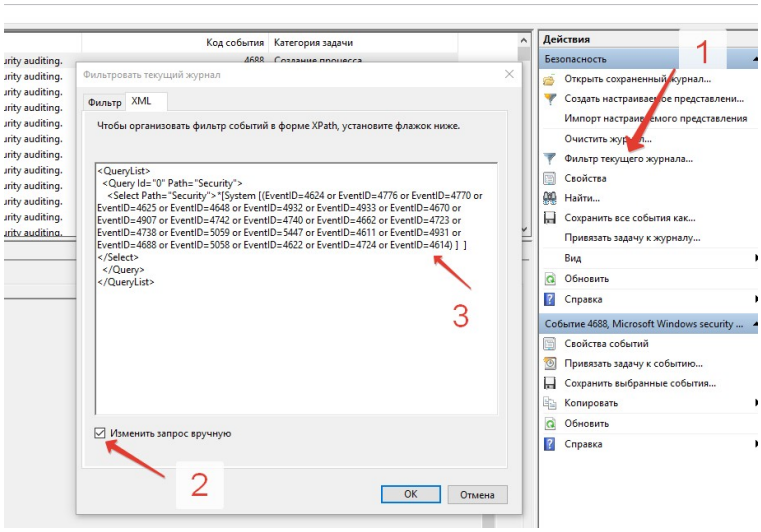


Рисунок 5.2 – Чекбокс «Изменить запрос вручную»

Обратите внимание, поскольку запрос вставляется внутрь XML, в нем надо экранировать символы <, > и & как <, > и & соответственно.

Следующий фильтр выводит все события, которые SID которых соответствует пользователю Local System:

*[EventData[Data[@Name="SubjectUserSid"] and (Data = "S-1-5-18")]]

Использование профиля WinEventLog не единственный способ сбора событий с операционной системы Microsoft Windows. Другие способы сбора информации – забрать журнал по протоколу WMI (модуль wmilog, системный профиль EventLog via WMI) или использование модуля wminotification (системные профили «Monitoring Windows CPU Load», «Monitoring Windows HDD Load», «Monitoring Windows RAM Load» и «WMI Notification»). Модуль предназначен для сбора событий WMI-классов по протоколу WMI. Подписка реализуется WQL- запросами. Описание этих профилей можно найти в документации (Operator Guide). Для сбора информации при помощи модуля «WMI Notification» полезно провести предварительную настройку конечных точек для сбора дополнительных событий полезных для обнаружения атак. Эти настройки можно осуществить при помощи групповых политик. Но если такой возможности нет, то можно воспользоваться скриптами PowerShell расположенными в системных справочниках src_setup_epm (для узлов, на которых установлен Endpoint Monitor) или src_setup_noepm (для узлов, на которых Endpoint Monitor не установлен). Для массового выполнения этих скриптов удобно создать задачу на основе профиля «Setup windows workstation for monitorig (EPM configuration)» – модуль remote-executor или профиля «Setup windows workstation for monitorig (no EPM configuration)» соответственно. Профиль «Rollback windows workstation to default monitoring settings» предназначен для отката сделанных изменений.

Часть 2. File via SSH

Цель:

Научиться собирать информацию с журналов Linux через SSH соединение.

Создайте задачу для мониторинга журнала аутентификации Linux. Используйте для этого модуль ssheventcollector. Это не лучший из возможных способов сбора журнальных данных. Суть метода состоит в том, что Agent проходит на Unix-машину при помощи ssh, повышает привилегии (если это необходимо) и выполняет в бесконечном цикле заданную команду, в нашем случае tail -n 2000 -f /var/log/auth.log. Все, что будет передавать эта команда на свой стандартный вывод (и стандартный поток ошибок), будет восприниматься как поток событий. Контроль корректности данных и контроль отсутствия повторов полностью отданы на совесть выполняемой команды. Строго говоря, эта команда совсем не обязательно должна непременно следить за содержимым какого-то файла, она может, например, следить при помощи команды who за пользователями, авторизованными в системе, температурой CPU, зарядом батарей ноутбуков или другими

интересными параметрами – при условии, что в системе есть подходящие правила нормализации для данных команд.

1. Для начала создайте свой профиль.

На вкладке «Сбор данных/Профили» выберите профиль «File via SSH» и сделайте его копию, нажав кнопку «Создать/На базе выбранного профиля».

Назовите профиль /var/log/auth.log via SSH. Здесь же, в настройках транспорта укажите учетные записи FirstLogin и SecondLogin для транспорта Terminal. И здесь же сконфигурируйте транспорт Terminal для настройки задачи. Эти действия упростят далее настройку задачи.

Название	/var/log/auth.log via SSH
Учетная запись First Login (необязательно)	Linux Auditor 1
Учетная запись Second Login (необязательно)	Linux Auditor 2

Нажмите кнопку «Параметры» и в поле «Команда для получения событий» напишите tail -n 2000 -f /var/log/auth.log

Команда для получения событий	tail -n 2000 -f /var/log/auth.log
Тонкая настройка источников событий	[{"input_id":"@GUID","time_delta":0,"time_zone":10800}]

Или перейдите на вкладку JSON и в нижнем окне переопределите опцию:

```
{
    "COMMAND": "tail -n 2000 -f
    /var/log/auth.log","inputs": [
        {
            "input_id":
            "@GUID",
            "time_delta": 0,
            "time_zone": 10800
        }
    ]
}
```

Нажмите значок шестеренки у вкладки Terminal и в параметрах транспорта сделайте следующие две настройки:

Тип локальной аутентификации Local authorization method	1
Метод повышения привилегий Privilage escalation method	1

Или перейти на вкладку JSON и в нижнем окне переопределить две опции:

```
{
    "SSH.AUTH_TYPE": 1,
```

"SSH.USE_ROOT_LOGON_TERMINAL": 1

}

Ниже, на трех скриншотах (Рис. 5.3, Рис. 5.4 и Рис. 5.5) проиллюстрирована настройка пользовательского профиля.

2. Сделаем задачу по сбору данных по аутентификации в Linux.

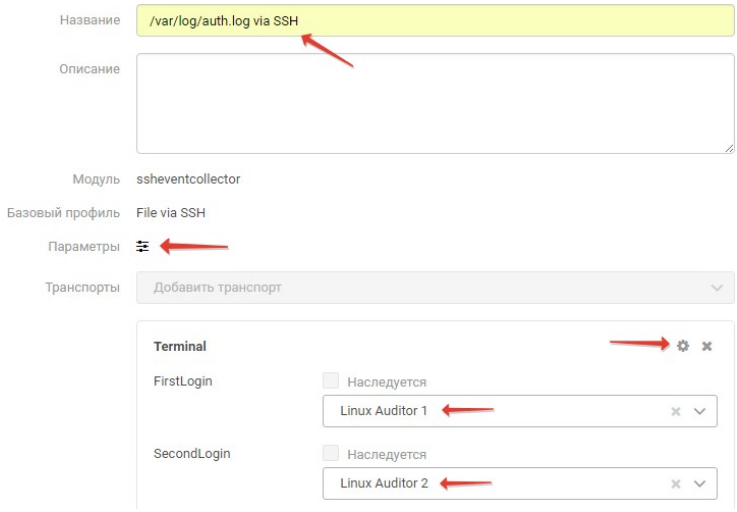


Рисунок 5.3 – Настройка пользовательского профиля /var/log/auth.log via SSH

Рисунок 5.4 – Настройка дополнительных параметров пользовательского профиля /var/log/auth.log via SSH

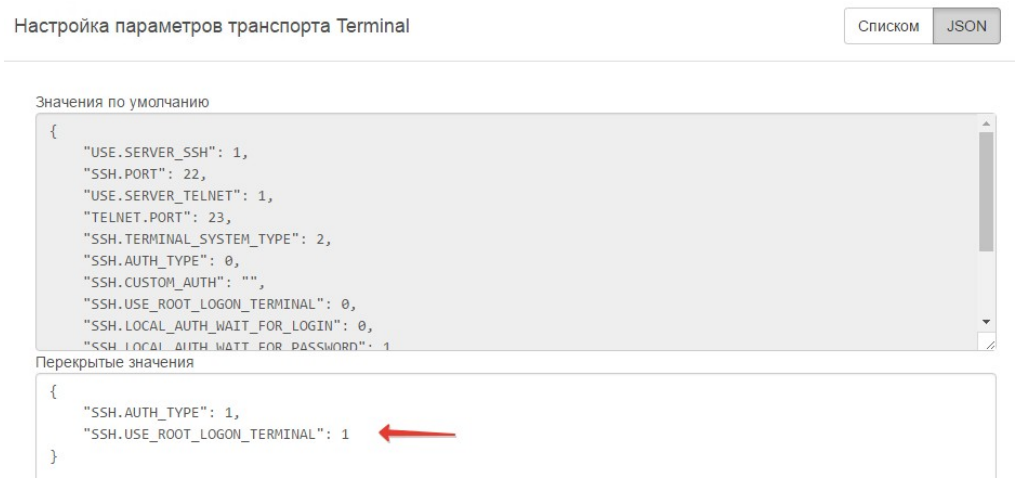


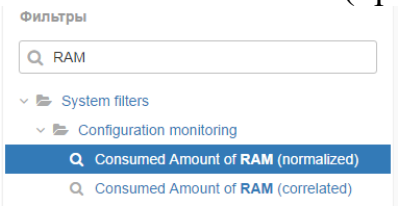
Рисунок 5.5 – Настройка параметров транспорта Terminal для пользовательского профиля /var/log/auth.log via SSH

Часть 3. Работа с событиями. Язык запросов PDQL

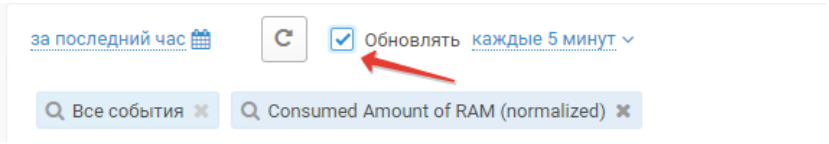
Цель:

Научиться создавать собственные фильтры событий с помощью встроенного языка PDQL.

1. На вкладке События/Просмотр событий найдите системный фильтр Consumed Amount of RAM (просто впишите слово RAM в окошко поиска).



2. Установите чекбокс «Обновлять каждые 5 минут» – события будут подгружаться автоматически.

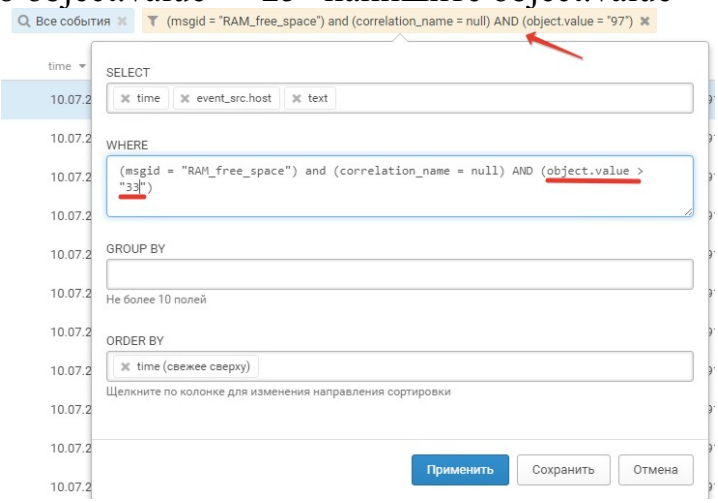


3. Чтобы увидеть события, сигнализирующие о том, что средняя загруженность RAM превышает 33%, модифицируйте запрос на PDQL следующим образом:

a. В правой части экрана, найдите поле object.value и щелкните по числовому значению.

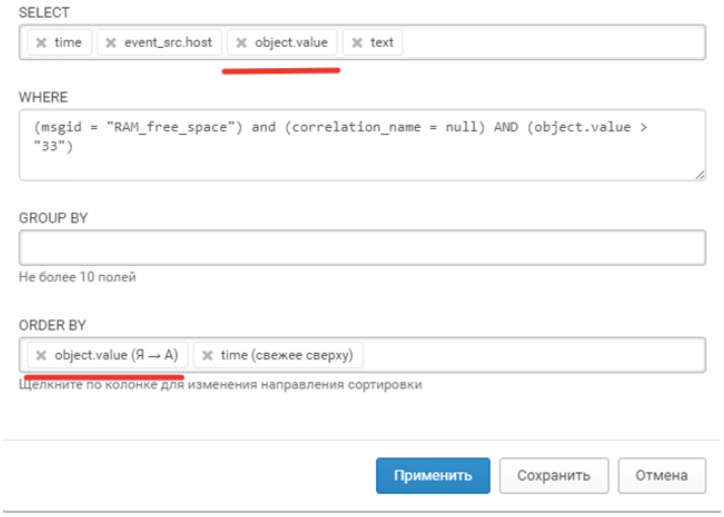
Здесь при помощи щелчка по одному из двух предопределенных фильтров вы можете автоматически добавить к текущему фильтру PDQL новое условие. Сделайте это.

b. Щелкнув по выражению на PDQL, вы увидите запрос, разделенный на поля. В поле Where найдите добавленное условие и отредактируйте его: вместо object.value = "25" напишите object.value > "33".



c. Чтобы не только увидеть узлы, на которых память использована более чем на 33%, но также иметь возможность сортировать узлы по убыванию загруженной памяти, добавьте поле object.value в поле Select и в

поле Order By. В поле Order By мышью перетащите поле object.value на первое место и кликните на нем, изменив направление сортировки с А↓Я на Я↓А.



4. Обратите внимание на возможную ошибку сортировки: 7% > 33%. Далее мы поймем причины этого явления и устраним его:

a. Откройте файл C:\Program Files\Positive Technologies\MaxPatrol SIEM Server\taxonomy.json в редакторе notepad++ и нажмите клавиши Alt+2. Вы увидите список полей таксономии. Найдите поле object.value и раскройте (кликните по значку с плюсиком).

"object.value": { "asset_resolution": false, "auto": false,

"class": "scalar", "filterable": true, "groupable": false, "selectable": true, "sortable": true, "type": "StringField"

},

Обратите внимание, поле object.value имеет строковый тип, поэтому сортировка в выборке алфавитная.

b. Для того, чтобы сортировка работала правильным образом, потребуем в PDQL, чтобы в поле object.value находилось двузначное число. Этого можно добиться одним из двух следующих способов:

i. (object.value > "33") AND match(object.value,"[0-9][0-9]")

ii. (object.value > "33") AND (object.value not in [4,5,6,7,8,9])

c. Завершая редактирование, вместо кнопки «Применить» нажмите кнопку

«Сохранить» и дайте новому фильтру название. Цвет фильтра изменится на голубой.

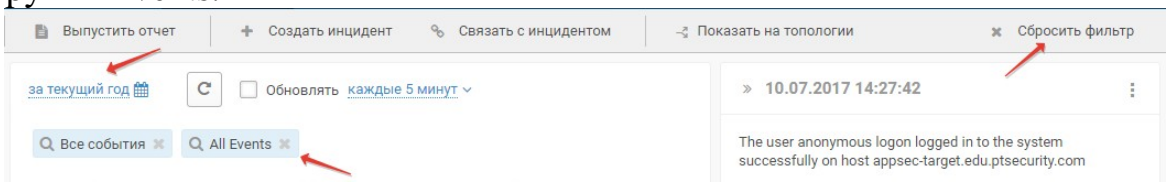
Часть 4. Группировка

Цель работы:

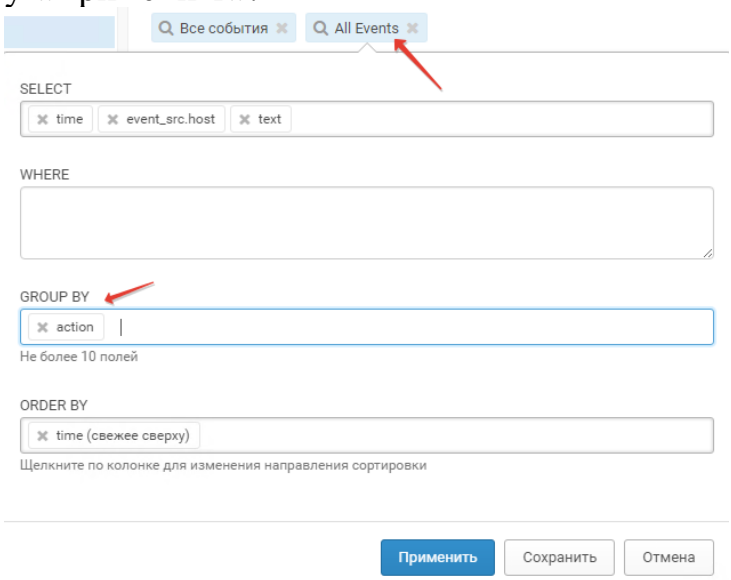
Научиться делать группировку и сортировку отфильтрованных результатов.

Начиная с релиза 16.0 группировка событий осуществляется в выражении PDQL при помощи оператора Group By.

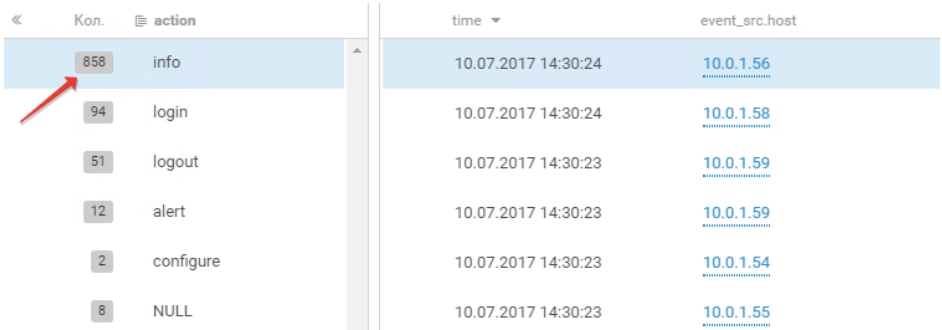
1. Сбросьте все фильтры (кнопка «Сбросить фильтр» справа сверху), установите временной период «текущий год» и кликните по системному фильтру All Events.



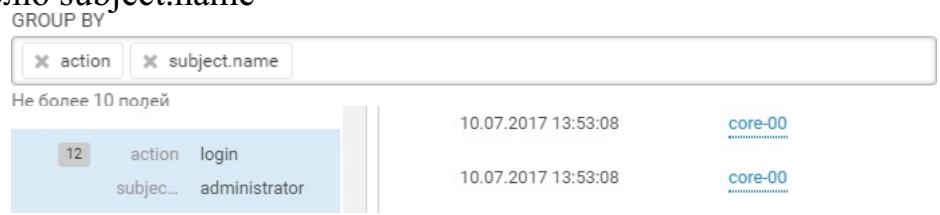
2. В поле Group By установите группировку по полю action и нажмите кнопку «Применить».



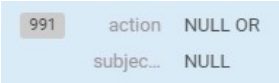
События будут сгруппированы по полю action. Вы увидите сколько событий с тем или иным значением поля action в указанном промежутке времени соответствовало выбаранному фильтру и сможете просматривать эти события



3. Группировки могут быть многоуровневыми (до десяти уровней). Попробуйте повторно войти в редактор PDQL и сделать вторую группировку по полю subject.name



Заметьте, поскольку в информационных событиях (где action=info) поля subject.name нет, то все такие события у нас попадут в группу action NULL OR subject.name NULL:



Задание. Работа с фильтрами PDQL

Цель: Освоение PD QL – языка запросов к базе событий

Найдите все попытки входа в различные системы от имени системных учетных записей компании Fortinet (логины начинающиеся со слова Forti).

Задание. Работа с модулем filemonitor, работа с фильтрами PDQL

Цель: Научиться загружать журналы в систему. Научиться находить и решать поблемы при помощи журнальных файлов. Освоение PDQL – языка запросов к базе событий. Получить навыки построения отчета о событиях.

Загрузите в SIEM события из файла auth.log (расположен на сервере RDS в папке Courseware for students\PT13 – SIEM\Exercise\auth.log). Для загрузки сделайте копию системного профиля WindowsFileLog. Инструкции по настройке модуля WindowsFileLog можно найти в документации (operatorguide, 13.1.2.5. Модуль filemonitor). При возникновении трудностей проверяйте журнал агента в папке C:\ProgramData\Positive Technologies\MaxPatrol SIEM Agent\log\modules\filemonitor. Журнал можно так же загрузить при помощи пользовательского интерфейса.

⚠Внимание! Правильный способ загрузки старого журнального файла – загрузка данных при помощи функции «Импорт журнала». Кнопка для создания профиля с импортом журнала в интерфейсе системы расположена там же, где и кнопка создания задачи. Однако в данной работе мы используем мониторинг за журналом, так как будто в этот журнал продолжает писать данные какой-то сервис. Мы делаем это в чисто образовательных целях. Начиная с релиза 17.0 опция skip_first_scan_result в модуле filemonitor выставляется по умолчанию в true. Это значит, что те строки что уже находятся в журнале, не будут подгружаться. Подгружаться будут только те записи, которые появились в журнале после старта задачи. Поэтому вам надо выставить эту опцию в false.

На узел example.com идут атаки SSH bruteforce. Когда служба sshd сталкивается с невозможностью пустить пользователя из-за того, что его нет в системе, она генерирует событие при нормализации которого в поле reason появляется сообщение Invalid user (или invalid user).

Найдите при помощи SIEM учетные записи, наиболее подверженные взлому. Найдите список IP- адресов, с которых идут атаки. Выпустите отчет со статистикой атак по пользователям.

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

Отчет должен включать:

– титульный лист;

– цель работы;

– ход работы, содержащий пошаговое описание осуществленных действий, иллюстрированных скриншотами на каждом этапе выполнения;

– вывод.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Практическая работа № 6

Тема. Организация охраны объектов

Цель занятия: Научиться определять тип событий (скоррелированное или нормализованное), понимать их различия. Просмотр сырых событий (т.е. событий попавших в нормализатор) и исходных событий вызвавших корреляцию.

Теоретическая часть:

Корреляции

Системные корреляции, имеющиеся в продукте удобно классифицировать по полям category.generic, category.high и category.low. Перечень значений этих категорий можно найти в документах OperatorGuide и DeveloperGuide.

Откройте вкладку Сбор данных / Правила корреляции и отсортируйте правила по столбцу «Категория». В учебном пособии список типов корреляций не полный. Заметьте, что здесь перечислены только правила корреляции, которые срабатывают в случае, если для обнаружения инцидента недостаточно просто увидеть какое-то событие, а надо соотнести событие с известной конфигурацией актива (модельные корреляции) или с другими событиями. Некоторые правила корреляции, наоборот, носят чисто служебный характер и не говорят о том, что что-то случилось.

Например, одно правило корреляции может заполнять табличный список информацией, которая окажется интересной другой корреляции. Последняя уже будет свидетельствовать об инциденте. Например: одна корреляция может записывать информацию о возможных жертвах bruteforce атак на оборудование Cisco, а другая будет срабатывать в том случае если от потенциально взломанной учетной записи отдали команду show run. В то же время, если важное событие порождается сразу нормализатором, а не коррелятором, то оно тоже будет иметь аналогичные поля category.generic, category.high и category.low.

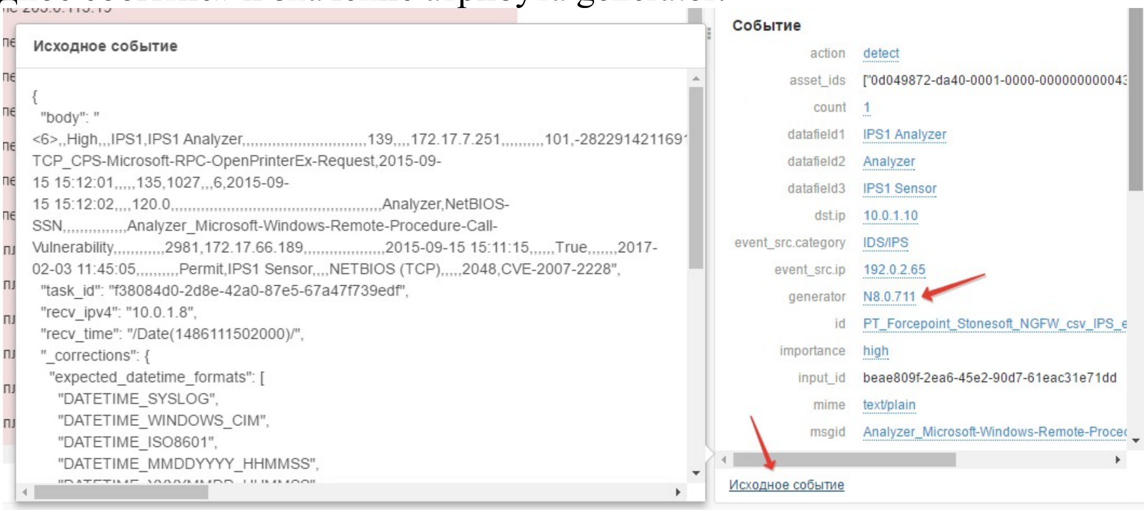
Таблица 6.1 – Обзор правил корреляций

Категория	**Описание**
Access / Authentication	События, касающиеся входа в систему: успешный или неуспешный вход в систему важного пользователя и т.п.
Accounting / User Accounting	События, связанные с критичным поведением пользователей: просмотр важных таблиц, выполнение критичных команд, запуск критичных транзакций и т.п.

Категория	Описание
Anomaly / Network Anomaly / Detection	Ненормальное поведение системы: Открыто слишком много TCP-соединений, запуск важных процессов после выхода из системы и т.п.
Anomaly / User Behavior Anomaly / Detection	Обнаружение странного поведения пользователей: создание учетной записи сразу после входа в систему, остановка антивируса или межсетевого экрана после выхода пользователя из системы и т.п.
Attack / Damage / Data corruption	Обнаружение факта работы шифровальщика
Attacks & Recon / Attack / Bruteforce	Разнообразные действия типа Bruteforce
Attacks & Recon / Recon / Enumeration	Проведение разведывательной деятельности. Например, в Unix пользователь отдал команду ls -R /, которая выводит рекурсивно содержимое всех каталогов и подкаталогов.
Compliance / Policy Violation / Application Policy Violation	Запуск запрещенного ПО, например TeamViewer
То же, но / IP Access Policy Violation	Тоже нарушение политик, но в отношение сетевого трафика, например попытка входа в коммутатор Cisco с «неправильного» актива
Configuration Management / Rights Management / Critical Privileges	Нарушения в конфигурации актива. Например создание временного администратора в Windows
Configuration Management / System Configuration Management / Network Service Modification	Нарушения в конфигурации актива. Например, изменение правилмежсетевого экранирования в Unix
Hacktool / Scanner / Exploitation	Запуск сканеров
Hacktool / Miscellaneous / Detection	Обнаружение хакерских инструментов в системе: mimikatz Cain&Abel и др.
Information Management / Data Loss / Deliberate	Массовое удаление файлов и каталогов
Malware / Miscellaneous / Detection	Обнаружение ВПО
Monitoring / System Monitoring / Performance или Processes	Все, что касается ресурсов системы: Нехватка ресурсов системы, недоступность службы или сетевого сервиса
Network Interaction / Network Interaction / VPN	События запуска и прекращения работы каналов VPN

Методические рекомендации по выполнению практического занятия

1. Откройте вкладку события. Найдите событие, пришедшее от источника (не результат корреляции), обратите внимание на наличие ссылки «Исходное событие» и значение атрибута generator.



2. Найдите все нормализованные события при помощи запросов PDQL:

a. correlation_name = null

или

b. match(generator,"N.*")

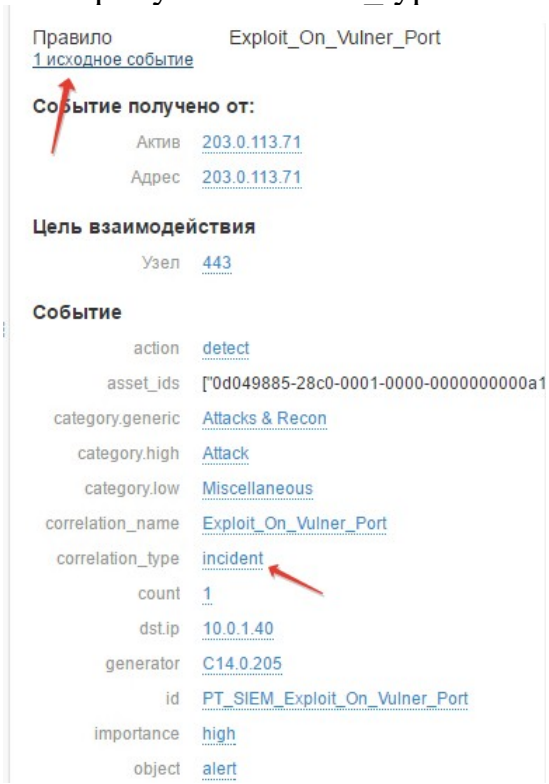
3. Найдите скоррелированные события при помощи запросов PDQL:

a. correlation_name != null

или

b. match(generator,"[CA].*")

4. Обратите внимание на ссылку, по которой можно обнаружить исходные события, на основании которых сделана данная корреляция, и на значение атрибута correlaton_type:



Атрибут correlation_type может принимать значение либо event, либо incident. В последнем случае формируется инцидент на вкладке «Инциденты».

Сбор событий по протоколу syslog

Цель: научиться собирать данные по протоколу syslog

1. Создайте задачу по сбору данных syslog. Данные по протоколу syslog на Агенты отправит преподаватель.

Название задачи	Get Syslog Messages
Профиль	Syslog
Агент	Выбрать из выпадающего списка

Запустите сценарий, эмулирующий работу клиента syslog и отправляющий события на узлы слушателей.

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

Отчет должен включать:

– титульный лист;

– цель работы;

– ход работы, содержащий пошаговое описание осуществленных действий, иллюстрированных скриншотами на каждом этапе выполнения;

– вывод.

Практическая работа № 7

Тема. Технологические меры поддержания информационной безопасности объектов

Цель занятия: Получить представление о процессе обработки инцидентов, научиться назначать ответственного и получать информацию о статусе обработки инцидентов.

Теоретическая часть:

Компонент SIEM

SIEM (Security information and event management, «управление событиями и информацией о безопасности») – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности.

SIEM – это, по сути, объединение классов SEM (Security Event Management, «управление событиями безопасности») и SIM (Security Information Management, «управление информацией о безопасности»). Решения SEM используются для мониторинга событий безопасности в реальном времени. Системы SIM, в свою очередь, отвечают за долгосрочное хранение и анализ данных с различных объектов инфраструктуры организации. SIEM-решения выполняют обе эти задачи.

Функциональность SIEM-систем

В задачи SIEM-систем входит:

1. В реальном времени отслеживать сигналы тревоги, поступающие от сетевых устройств и приложений.
2. Обрабатывать полученные данные и находить взаимосвязи между ними.
3. Выявлять отклонения от нормального поведения контролируемых систем.
4. Оповещать операторов об обнаруженных инцидентах.

В классическом понимании SIEM-системы только собирают и обрабатывают данные, а также оповещают оператора о возможной опасности. Блокирование подозрительных процессов, помещение файлов на карантин и прочие меры реагирования в их задачи не входят. Однако в последнее время под термином SIEM часто объединяют как системы сбора и обработки данных, так и системы, позволяющие затем реагировать на полученную информацию и предпринимать активные действия.

Применение SIEM-решений

При помощи SIEM ИБ-специалисты могут выявить кибератаки и нарушения политик безопасности на ранних стадиях и минимизировать ущерб от них. Также решения SIEM помогают оценить защищенность

информационных систем и актуальные для предприятия риски. Кроме того, полученные от SIEM-систем данные используются при расследовании инцидентов и для формирования отчетности.

Сбор данных в SIEM-системах

Решения SIEM могут собирать данные о событиях безопасности четырьмя способами: с помощью специальных приложений (этот метод используется чаще всего), напрямую из файлов с логами, напрямую с сетевых устройств или с помощью протоколов потоковой передачи данных, например SNMP, Netflow или IPFIX.

В качестве источников информации для SIEM-решений могут выступать:

- антивирусные программы;
- системы авторизации и аутентификации;
- межсетевые экраны, брандмауэры;
- журналы сетевого оборудования, серверов и рабочих станций;
- контроллеры домена;
- системы обнаружения и предотвращения вторжений (IDS/IPS);
- системы предотвращения утечки информации (DLP);
- решения для контроля активов и инвентаризации.

На рисунке 7.1 схематично представлен Компонент Siem.

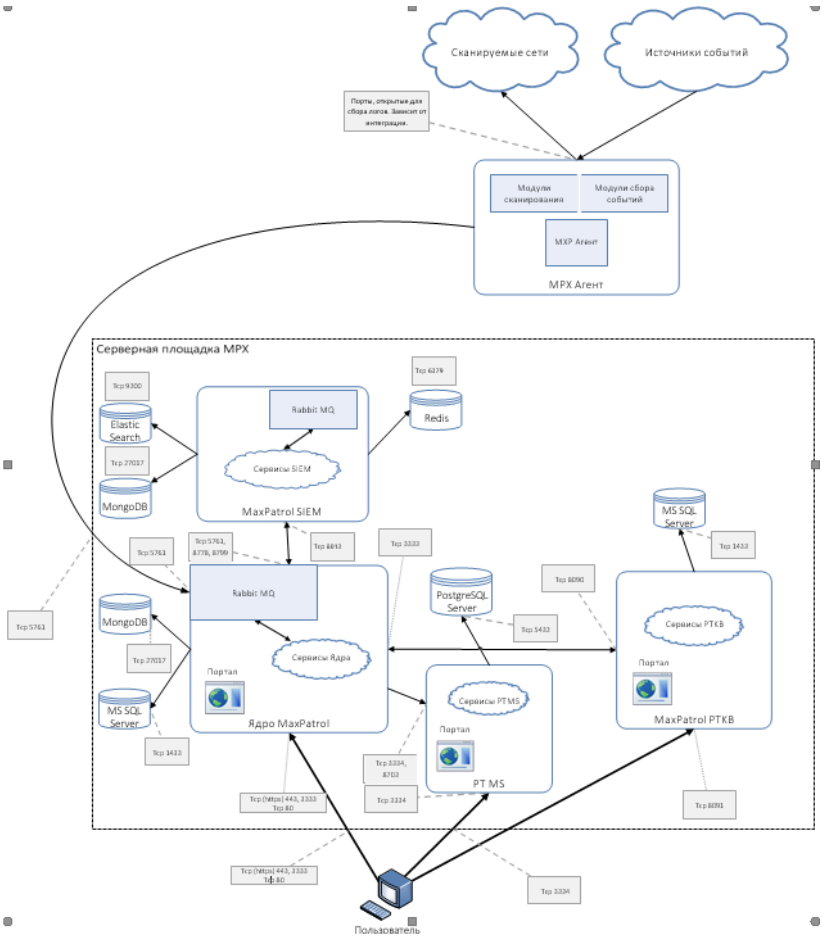


Рисунок 7.1 – Схема Компонент Siem

Компонент Siem подписан на очередь событий от источников. Эти события (так называемые raw- события – обернутые в JSON-конверт события от агента, пришедшие через RMQ-Host) Siem подвергает нормализации, корреляции и агрегации. Все события (как исходные raw, так и нормализованные, и результаты корреляции) Siem помещает в базу данных Elasticsearch. Данная база также не обязана находиться на одном узле с Siem. По соображениям производительности и отказоустойчивости база Elasticsearch может располагаться на внешнем кластере. Для работы так называемых модельных корреляций (корреляций, учитывающих строение информационной системы) Siem может обращаться к ядру как к AssetResolverHost за информацией об активах.

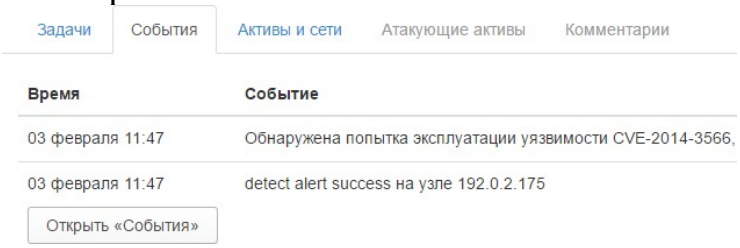
Методические рекомендации по выполнению практического занятия

Часть 1. Работа с автоматически созданным инцидентом

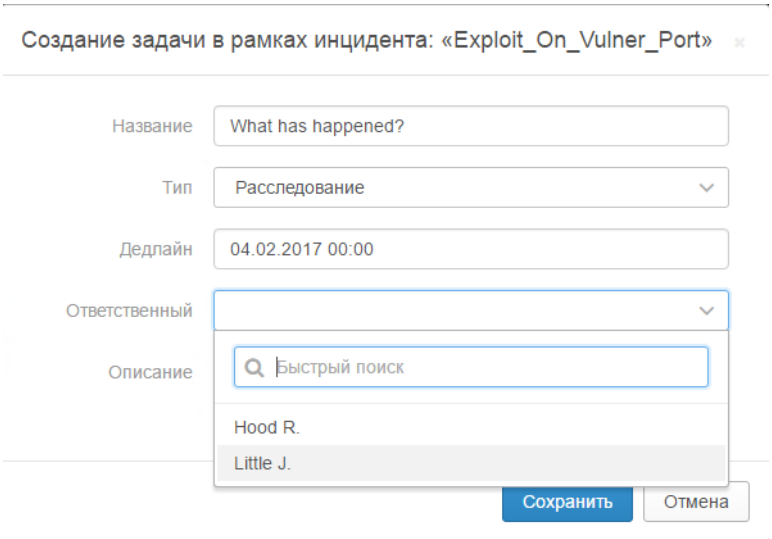
Цель:

Научиться постановке задач на инцидент и назначать ответственного. Познакомиться с процедурой смены статуса у задач. Научиться отправлять уведомления ответственным сотрудникам.

1. Откройте вкладку с инцидентами и пройдите в один из инцидентов. На вкладках «События» и «Активы и сети» изучите приведенную там информацию. Откройте список исходных событий для данного инцидента по кнопке «Открыть События».



2. Вернитесь на вкладку «Задачи» описания инцидента и поставьте задачу на расследование инцидента одному из сделанных ранее пользователей.

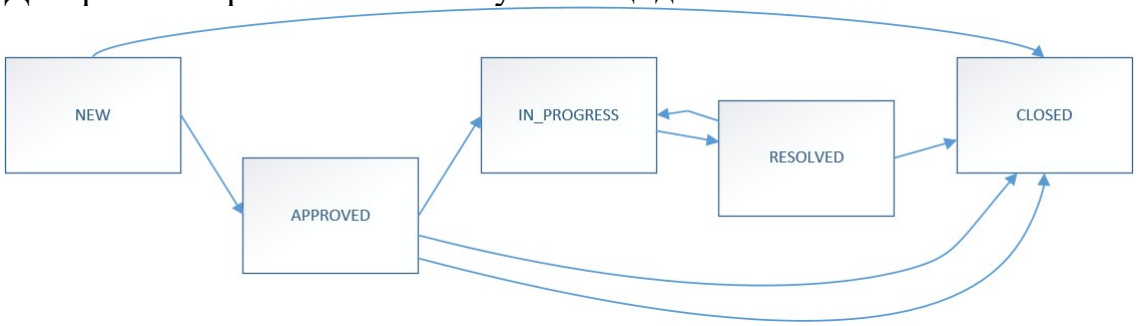


3. Зайдите в систему этим пользователем (удобно воспользоваться для этого режимом браузера «Инкогнито»). На вкладке Инциденты/Задачи будет видна созданная задача.

4. Измените задаче статус на «Закрыта».

5. Обновите окно с описанием инцидента – задача перейдет в список закрытых.

Диаграмма переключения статусов инцидента:



6. Перейти на вкладку Система/Уведомления и создать новое уведомление.

Название	Notify responsible person
Сообщать о состоянии	Инцидентов
Кому	Ответственный
По шаблону	Шаблон инцидентов по умолчанию
Периодичность	При каждом изменении

7. Назначить пользователя odminko (Little John) ответственным за какой-то инцидент. Изменить статус этого инцидента на «Утвержден» и поставить задачу типа «Расследование» с ответственным odminko (Little John).

8. Проверить почту odminko на сервере Core.

ⓘ Заметьте, нигде не указано, что почту должен получать odminko, он получает ее потому, что он назначен ответственным за инцидент, а в настройках уведомления сказано, что почту должен получать ответственный.

9. Перейти на вкладку Система/Уведомления и создать новое уведомление.

Название	Any events
Сообщать о состоянии	Событий
В группах	Все события (или другое на выбор)
Фильтр	All Events (или другое на выбор)
Кому	Little John

10. Проверить почту odminko на сервере Core.

Часть 2. Ручное создание инцидента

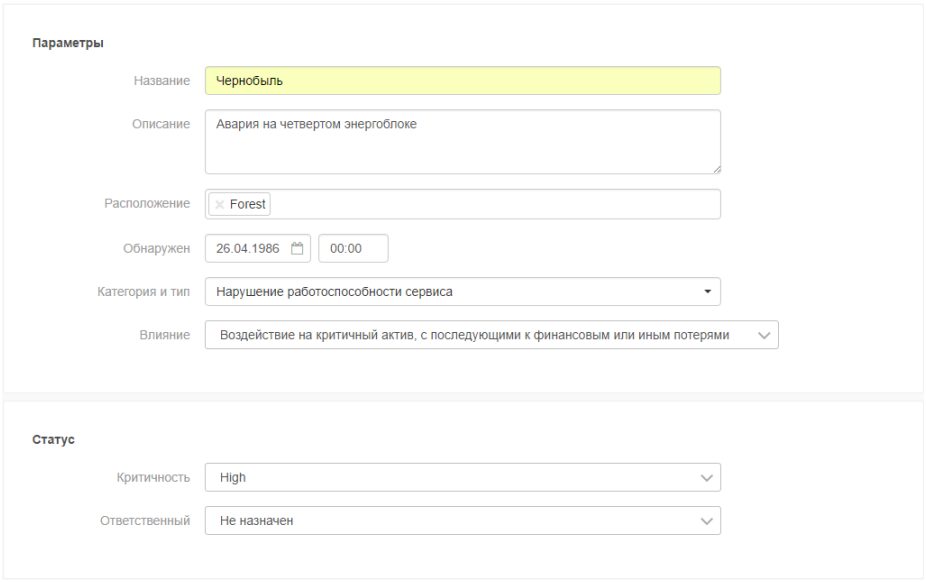
Цель:

Научиться создавать инцидент вручную.

1. На закладке Инциденты нажмите кнопку «Создать» и опишите инцидент.

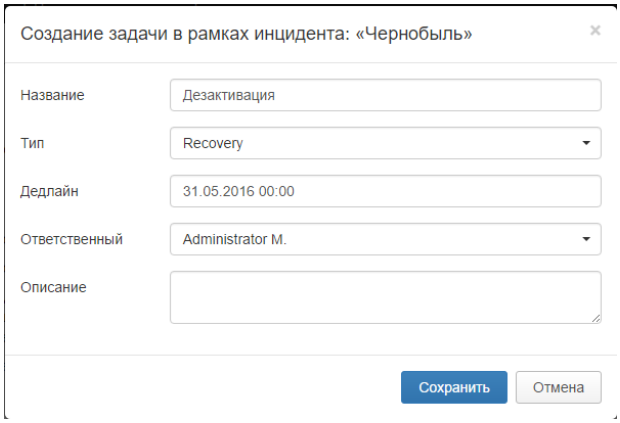
Название инцидента	Чернобыль

Расположение	Forest
Обнаружен	26.04.1986 0:00
Категория и тип	Нарушение работоспособности сервиса
Влияние	Воздействие на критичный актив…
Критичность	High
Ответственный	Не назначен



2. Сохраните инцидент. Номер ему будет присвоен автоматически.
3. В карточке инцидента вы создайте задачу в рамках отработки инцидента.

Название инцидента	Дезактивация
Тип	Recovery
Дедлайн	31.5.2016 00:00
Ответственный	Administrator M.



4. Нажав По кнопке «Изменить статус» вы можете переводить статус из состояния New в иные состояния.

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

Отчет должен включать:

– титульный лист;

– цель работы;

– ход работы, содержащий пошаговое описание осуществленных действий, иллюстрированных скриншотами на каждом этапе выполнения;

– вывод.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Практическая работа № 8

Тема. Организация контрольно-пропускного режима

Цель занятия: Научиться работать со статистической информацией. Научиться конфигурировать виджеты статистики.

Теоретическая часть:

Принцип работы систем SIEM

Понятие SIEM (Security Information and Event Management) в наши дни достаточно размыто, можно представить, что это процесс, объединяющий сетевую активность в единый адресный набор данных. Сам термин был придуман Gartner в 2005 году, но с тех пор само понятие и все, что к нему относится, претерпело немало изменений. Первоначально аббревиатура представляла собой комбинацию двух терминов, обозначающих область применения ПО: SIM (Security Information Management) – управление информационной безопасностью и SEM (Security Event Management) – управление событиями безопасности.

По утверждению Gartner, SIEM-система должна собирать, анализировать и представлять информацию из сетевых устройств и устройств безопасности. Также в эту систему должны входить приложения для управления идентификацией и доступом, инструменты управления уязвимостями и базы данных и приложений.

Для наглядности мы выделим несколько функций, которые обычно поставляются SIEM-системами:

- Возможность отправки предупреждений на основе предопределенных настроек.
- Отчеты и логирование для упрощения аудита.
- Возможность просмотра данных на разных уровнях детализации.

SIEM собирает логи разных приложений, обрабатывает и кладет в централизованное хранилище, с которым удобно работать.

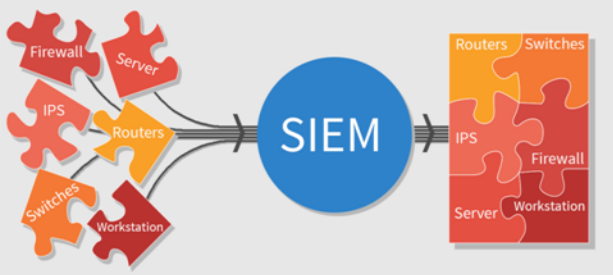


Рисунок 8.1 – Принцип сбора и хранения логов в SIEM

Как правило, размер хранилища зависит от количества обрабатываемых событий в сети компании. Из лидеров мирового рынка SIEM можно выделить следующих:

HP ArcSight
IBM QRadar SIEM
Tibco Loglogic
McAfee NitroSecurity
RSA Envision Splunk
LogRhythm

Есть и российские SIEM-системы:

MaxPatrol SIEM от Positive Technologies
КОМРАД от «НПО «Эшелон»
RUSIEM

SIEM в качестве улучшенной системы обнаружения вторжений

По словам некоторых экспертов, SIEM представляет собой улучшенную систему обнаружения вредоносной активности и различных системных аномалий. Работа SIEM позволяет увидеть более полную картину активности сети и событий безопасности. Когда обычные средства обнаружения по отдельности не видят атаки, но она может быть обнаружена при тщательном анализе и корреляции информации из различных источников. Поэтому многие организации рассматривают использование SIEM-системы в качестве дополнительного и очень важного элемента защиты от целенаправленных атак.

Рисунок 8.2 – Функции SIEM-системы

Типовые сценарии использования SIEM-системы

Отслеживание аутентификации и обнаружение компрометации аккаунтов пользователей и администраторов.

Отслеживание случаев заражения.

Обнаружение вредоносных программ с использованием исходящих журналов брандмауэра и журналов веб-прокси, а также внутренних журналов подключения и сетевых потоков.

Мониторинг подозрительного исходящего трафика и передаваемых по сети данных с использованием журналов брандмауэра, журналов веб-прокси и NetFlow.

Обнаружение кражи данных и других подозрительных внешних соединений.

Отслеживание системных изменений и других административных действий во внутренних системах и их соответствия разрешенной политике.

Отслеживание атак на веб-приложения и их последствий с использованием журналов веб-сервера, WAF (Web Application Firewall, экран для защиты веб-приложений) и логов приложений.

Обнаружение попыток компрометации веб-приложений путем анализа разных отчетов.

Так ли необходима SIEM-система?

Некоторые компании задаются вопросом, актуальны ли SIEM-системы или же этот подход уже устарел. Для ответа на этот вопрос необходимо понять, как следует использовать SIEM. SIEM не будет противодействовать хакерам, это решение для мониторинга, которое совершенствуется по мере развития технологии. Более того, без SIEM невозможно построить такие системы и центры мониторинга и реагирования, как SOC (Security Operation Center) и подключиться к FinCert или ГосСОПКА, так как SIEM помогает решать целый ряд ключевых задач: собирать и хранить лог-файлы в едином централизованном хранилище, предоставлять специализированные отчеты аудиторам для соответствия требованиям законодательства и отраслевым стандартам и выполнять корреляцию событий между различными источниками. Следует уделить особое внимание настройке SIEM под клиента, его инфраструктуру и системы безопасности. Хорошо настроенные правила корреляции позволят оператору анализировать действительно важные сообщения об инцидентах, отсеивая лишнее.

Методические рекомендации по выполнению практического занятия

Часть 1. Статистика

Цель:

Научиться работать со статистической информацией. Научиться конфигурировать виджеты статистики.

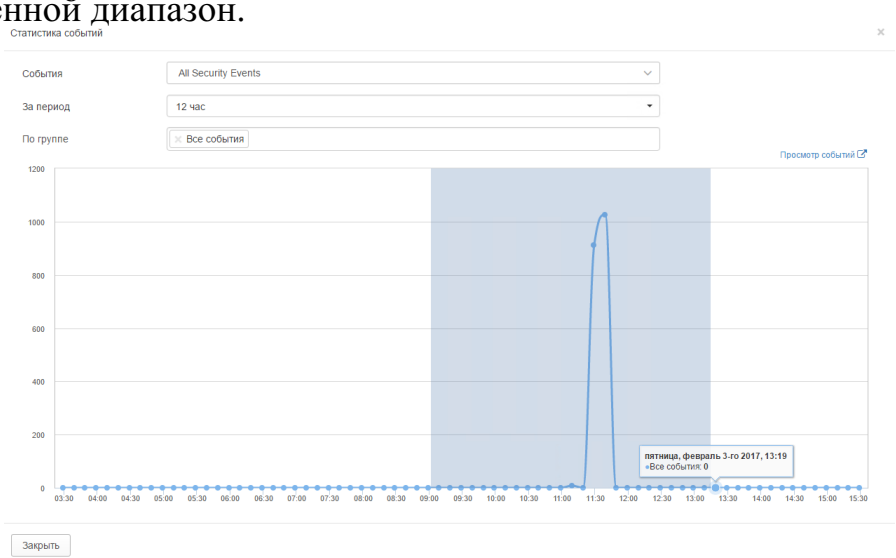
1. Перейдите на вкладку «Активы/Статистика». Здесь найдите информацию о том, когда и сколько просканировано узлов, информацию о самых уязвимых узлах, о распределении уязвимостей по узлам. Обратите внимание как можно выводить эту сводную информацию по группам активов.

Внимание! Если вы сканировали сеть в тот же день, когда осуществляете эту лабораторную работу, то есть сегодня, вы можете столкнуться с отсутствием информациив виджетах. Обратите внимание, что уязвимости выводятся по умолчанию по состоянию на 0 часов, 00 минут. В это время сегодня информации и в самом деле не было. Выставите корректное время, и все заработает. Переключая время, вы можете видеть, как менялась картина с уязвимостью с ходом времени.

2. Перейдите на вкладку «События/Статистика». Здесь вы видете шесть виджетов с отображением распределения событий во времени. Виджеты отличаются фильтрами, которые можно выбрать из выпадающего меню. В том числе можно выбрать пользовательские фильтры, написанные вами на PDQL и сохраненные на вкладке «События/Просмотр событий».

3. Воспользуйтесь ссылкой «Просмотр событий».

4. Нажмите кнопку «Увеличить» и выделите мышью на графике временной диапазон.



5. Аналогично изучите вкладку «Инциденты/Статистика».

6. Откройте вкладку Система/Мониторинг SIEM. Здесь на трех вкладках можно найти виджеты, описывающие во времени, с каких модулей события приходили в систему, как работает служба нормализации событий. Много ли событий не нормализовано, как работает коррелятор.

В настоящее время диаграмма «Статистика работы нормализатора» – единственное место в UI системы MaxPatrol SIEM, где можно увидеть информацию о ненормализованных событиях. Остальная информация о том, какие события не нормализуются и много ли событий, которые не может обработать хранилище, можно найти непосредственно в базе Elastic Search и в интерфейсе шины данных RabbitMQ при помощи отладочных инструментов

Часть 2. Построение отчетов

Цель:

Получить представление о вариантах составления отчетов. Научиться создавать отчеты.

1. Напишите выражение на PDQL, выводящее все события, произошедшие на узле example.com, в которых было действие login (неважно, успешное или нет).

2. Сузьте временные рамки до периода с 4 по 11 мая.

3. Нажмите кнопку «Выпустить отчет» и выпустите отчет «Статистика событий по пользователям» в формате PDF.

4. Перейдите на вкладку Активы, выделите группу Vulnerable OpenSSL и постройте отчеты «Инвентаризация Shares» и «Инвентаризация Shares по узлам» в формате PDF. Изучите отчеты. Посмотрите, какие еще отчеты могут быть вам полезны.

5. Изучите возможность создания отчета по расписанию. Для этого либо перейдите на вкладку «Система/Отчеты по расписанию» и нажмите кнопку «Создать», либо из диалога настройки отчета (см. предыдущий пункт) нажмите кнопку «Создать отчет по расписанию». В этом случае вы попадете на ту же вкладку, но диалог создания отчета будет уже заполнен.

Задание. Отчеты

Цель: Научиться создавать отчеты в формате Excel, для последующего анализа данных.

Создайте файл в формате Excel, в котором будут выгружены все события с действием login, которые пришли в систему при помощи модуля filemonitor с машины core. Файл должен содержать три столбца: время события, логин и результат (success или failure). Таблица должна быть отсортирована по столбцу с результатом логина.

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

Отчет должен включать:

– титульный лист;

– цель работы;

– ход работы, содержащий пошаговое описание осуществленных действий, иллюстрированных скриншотами на каждом этапе выполнения;

– вывод.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Практическая работа № 9

Тема. Правовые механизмы информационной безопасности Российской Федерации

Цель занятия: Научиться правильно обращаться в техническую поддержку вендора для сокращения сроков обработки запроса путем предоставления необходимых, для понимания происходящего, данных.

Теоретическая часть:

Методология сравнения SIEM-систем

На этапе выбора критериев сравнения в нашей рабочей группе возникали жаркие споры насчет корректности сравнения существующих решений (а рассматриваются далеко не все присутствующие на рынке) или недостаточного раскрытия ряда функциональных возможностей. И тут действительно нужно пояснить: пути развития выбранных нами для сравнения SIEM-систем имеют разные длину (в годах) и направление – поэтому оценивать нужно потенциальному заказчику, основываясь на особенностях своей организации.

Например, потребности сервисного SOC, продающего свои услуги другим компаниям, разительно отличаются от потребностей инфраструктурного внутреннего SOC. И если для первого важно подключить из коробки максимальное количество источников и иметь возможность гибкого управления данными, поступающими от них, то для второго большим приоритетом может стать удобный пользовательский интерфейс и минимальная стоимость владения решением.

И если особенности заказчика формируют потребности, то функциональность продуктов определяет их возможности. Это ориентировка на интеграцию внутри собственной экосистемы, как у Positive Technologies и IBM, или направленность на интеграцию со сторонними решениями, как у RuSIEM и Micro Focus Security. Кроме того, подходы к визуализации и навигации в консоли каждого из решений соответствуют определенной логике, которую не всегда можно оценить четкими критериями, но зато можно эмпирически принять при живой демонстрации.

Группировка критериев осуществляется на основе базовых влияющих на компании-потребители направлений, диктуемых временем: степень автоматизации, стратегия развития (в том числе устойчивость на рынке), эластичность архитектуры. Возможность компании-потребителя учитывать риски при таких условиях в дальнейшем определяет ее выбор.

К примеру, небольшим игрокам стоит присмотреться к комплексному моновендорному решению, а тем, кто крупнее, ориентироваться на нишевые (под нишей подразумевается отрасль) решения.

Для создания полезного инструмента выбора были выделены следующие группы критериев сравнения SIEM-систем:

Архитектура решения – форм-фактор, масштабируемость, методы управления событиями и схема лицензирования – важный параметр для Enterprise-установок, где необходимо подсчитать конечную стоимость владения решением, учитывая трудоемкость обслуживания, возможность и эффективность реализации в распределенных сетях.

Общая информация – будет полезна при презентации руководству или организации референс-визитов, соответствия основных показателей ИТ- и ИБ-стратегии компании. По этим показателям можно судить о зрелости решения и его положении на рынке.

Функциональные особенности –наличие и составляющие кастомизируемых параметров, гибкость настройки позволят оценить

применимость решения к принятой парадигме развития процессов обеспечения ИБ (аутсорсинг, централизованное, распределенное использование) компании. А качество и количество предустановленных из коробки элементов, а также среднее время старта дадут представление о сроках внедрения до получения первых показателей эффективности.

Интеграционные возможности – наличие развитых встроенных и интегрируемых подсистем управления уязвимостями, инцидентами и активами позволит в начальном периоде эксплуатации ограничиться использованием одного продукта, без увеличения количества используемых администратором и аналитиком консолей. А интеграция со сторонними решениями в целях обогащения информации о событиях ИБ, сведения об API и поддерживаемых источниках событий указывают на открытую позицию компании на рынке, умение находить общий язык с другими игроками, говорит о направлениях развития продукта.

Дополнительные критерии – параметры, которые подвержены влиянию внешней среды. Это и отчетность, удобство, это и глубина погружения при навигации в рамках интерфейса системы. Все это влияет на оперативность при обработке событий ИБ и выявлении инцидентов ИБ и позволяет примериться к существующим внутри компании KPI. Дорожные карты развития, наличие озвученных планов по разработке коннекторов-парсеров, количество внедрений и поддержка со стороны производителя, а также живость community говорит о заинтересованности в продукте как заказчиков, так и разработчиков.

Соответствие направлению импортозамещения – позволит оценить ценность решения как компонента системы соответствия.

Методические рекомендации по выполнению практического занятия

Обсудите с преподавателем содержимое следующих каталогов:

Журналы агента:

C:\ProgramData\Positive Technologies\MaxPatrol SIEM Agent\log C:\ProgramData\Positive Technologies\MaxPatrol SIEM Agent\log\modules\

Журналы ядра:

C:\ProgramData\Positive Technologies\MaxPatrol SIEM Core\Logs

Журналы SIEM:

C:\ProgramData\Positive Technologies\MaxPatrol SIEM Server\log C:\ProgramData\Positive Technologies\MaxPatrol SIEM Server\normalizer\logs C:\ProgramData\Positive Technologies\MaxPatrol SIEM Server\correlator\logs C:\ProgramData\Positive Technologies\MaxPatrol SIEM Server\aggregator\logs C:\ProgramData\Positive Technologies\MaxPatrol SIEM Server\resolver\logs C:\ProgramData\Positive Technologies\MaxPatrol SIEM Server\rester\logs C:\ProgramData\Positive Technologies\MaxPatrol SIEM Server\router\logs C:\ProgramData\Positive Technologies\MaxPatrol SIEM Server\storage\logs

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

Отчет должен включать:

– титульный лист;

– цель работы;

– ход работы, содержащий пошаговое описание осуществленных действий, иллюстрированных скриншотами на каждом этапе выполнения;

– вывод.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

Практическая работа № 10

Тема. Правовое регулирование отдельных видов информации

Цель занятия: ознакомиться с существующим программным обеспечением для пассивного сбора информации об организации, получение практических навыков в пассивном сборе информации, анализ существующих методов и средств пассивного сбора информации.

Теоретическая часть:

Теория пассивного анализа

Пассивный анализ сети может быть обнаружен гораздо легче, но, несмотря на это, такой метод используется наиболее широко. Пассивные методы могут отображать соединения, определять порты и службы, используемые в сети, и даже могут определить операционные системы. Ланс Спицнер из Honeynet project и Майкл Залевский помогли инициировать разработку технологии *passive fingerprinting,* которая достоверно определяет операционные системы из трассировки TCP/IP. ПО p0f v 2.0.8, разработанное Залевским, является одним из самых эффективных инструментов пассивного опеределения ОС с помощью технологии fingerprinting.

Ключом для понимания методов пассивного анализа сети является понимание того, что они работает почти так же, как и активные методы построения карт. Все пассивные методы основываются на сценарии «запрос-ответ», они полагаются на чужой запрос, а затем собирают ответы (рисунок 10.1).

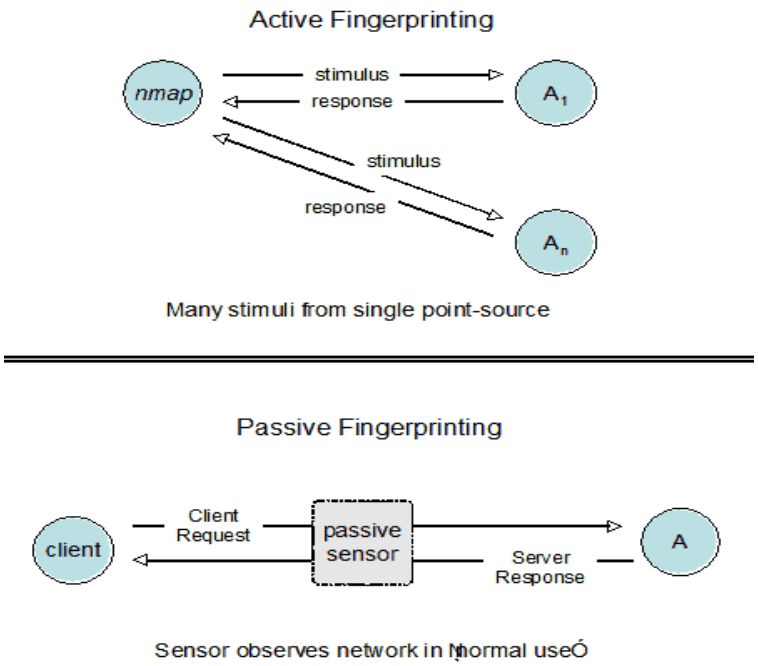


Рисунок 10.1 – Active and Passive Network Analysis

В активном сценарии объект (A) отвечает на запрос приложения, который строит карты сети, что является эффективным, но для этого примера мы создали искусственные условия наблюдения. В пассивном сценарии объект (A) отвечает на запросы в результате нормального функционирования. В обоих случаях мы получаем данные об используемых портах и службах, потоках соединений, информацию о времени, по которым можно сделать предположение о рабочих характеристиках нашей сети. Но пассивный метод позволяет также сделать то, что невозможно сделать с помощью активного метода: мы можем видеть сеть с точки зрения пользователя и изучать поведение приложений в ходе обычных операций.

Пассивный метод имеет несколько преимуществ по сравнению активным методом сканирования. Пассивные методы не генерируют трафик при мониторинге сети, что может иметь важное значение для сетевых приложений или в случаях, когда сеть не способна обработать большие объемы информации, передаваемые по сети при сканировании. Пассивные методы не генерируют предупреждения систем обнаружения атак и журналы записей в хостах и серверах при мониторинге сети, сокращая общую аналитическую нагрузку. В некоторых случаях пассивный метод анализа может выявить наличие брандмауэров, маршрутизаторов и NAT коммутаторов, и, возможно, охарактеризовать хосты, находящиеся за ними.

Несмотря на все преимущества, связанные с пассивными методами, у него есть и недостатки. Для проведения пассивного анализа всегда требуется вставить аппаратный или программный датчика в исследуемую сеть. Датчики должны быть размещены в топологии сети так, чтобы через них проходил полезный трафик, что является не тривиальной задачей в современных коммутируемых сетях. И наконец, инструментарий для пассивного анализа гораздо менее развит, чем традиционные методы активного анализа, т.к.

требуют значительных усилий от аналитика для размещения датчиков, сбора данных и анализа результата.

Чтобы лучше понять пассивный метод анализа, давайте изучим пример захвата с использованием Ethereal. Такой же результат можно получить, используя tcpdump, если вы умеете писать BPF-выражения (Berkley Packet Filters). Ethereal предлагает множество инструментов, которые позволят сэкономить время ленивым, включая улучшенные возможности фильтрации и быструю сортировку собранных пакетов по практически любым полям данных. Конечно, до начала сбора трафика и настройки фильтра полезно иметь представление о том, что мы ищем, в частности - о службах, используемых в нашей сети. К счастью, есть несколько настроек, позволяющих сделать это немного проще. Во-первых, большинство служб связаны с определенным портом. Эти "стандартные" порты назначаются IANA (Internet Assigned Numbers Authority) и описаны в RFC для стандартных TCP / IP служб и протоколов. Малоизвестные или используемые злоумышленниками порты могут быть исследованы с использованием Internet Storm Center [8], предоставленного SANS Institute. Оба ресурса обеспечивают отличное изучение материалов для общего анализа сети в целом, а также показывают, как другие администраторы безопасности сети анализируют свои сети.

Другое правило при анализе трафика позволяет разделить клиентов и серверы. Вообще говоря, серверы отправляют пакеты на номер порта, связанный со службой. Поэтому, найдя Web-сервер, вы смотрите на источник TCP-запроса на 80-ый порт, исходящий из вашей сети. Чтобы продемонстрировать это, я захватил трафик из моей домашней сети с помощью Ethereal и отсортировал его по портам TCP-запроса. Меня интересовало наличие веб-сервера, в чем я и убедился, отсортировывая захваченный трафик по 80 порту. Заметим, что наш датчик не инициировал трафик внутри сети. Чтобы получить результат, пакеты были сняты с канала. Я мог бы добиться того же результата, используя nmap, но это потребовало бы инициализации трафика в сети. Обращу ваше внимание – не все протоколы TCP подчиняются этому правилу, это исследование копии TCP / IP Illustrated!

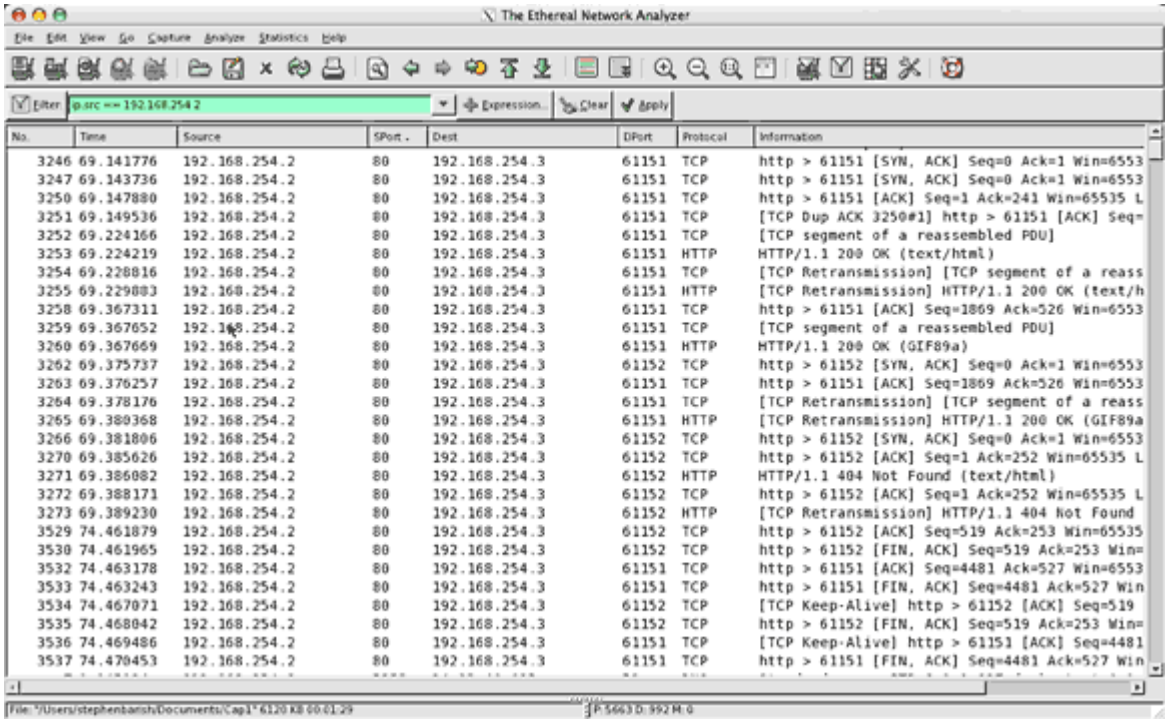


Рисунок 10.2 – Перехват трафика веб сессии, используя Ethereal

Благодаря тому, что TCP/IP fingerprinting работает в пассивном режиме почти также, как и в активном, мы можем выдвинуть некоторые гипотезы об операционных системах, используя системы перехвата трафика. Этот метод работает, потому что различные операционные системы имеют разные реализации TCP / IP стека. Программа Залевского p0f 2.0 расширяет эти параметры, позволяя проводить гораздо более точных тестов для выявления операционных систем в пассивном режиме (рисунок 10.3).

При повторном запуске p0f для захваченного ранее трафика мы определяем вебсервер как систему FreeBSD 6.x для данного Web сервера.

```
$ sudo p0f -s capture1.pcap -A
<Fri Aug 24 18:33:17 2007> 192.168.254.2:80 -
FreeBSD 6.x (2) [high throughput] (up: 715 hrs)
```

Operating System	WSS	Initial TTL	DF	SYN Size	Options[1]	Otions Expanded
Linux Kernel 2.0.3x on Mac	2	64	0	44	M*	MSS
Linux Kernel 2.6	4 x MSS	64	1	60	M*,S,T,N,W5	MSS, Selective ACK OK, Timestamp, NOP, Window Scaling 5
Solaris 9.1	32850	64	1	64	M*,N,W1,N,N,T,N,N,S	MSS, NOP, Window Scaling 1, NOP, NOP, Timestamp, NOP, NOP, Selective ACK OK
Windows XP SP1+	64512	128	1	48	M*,N,N,S	MSS, NOP, NOP, Selective ACK OK
Windows 2003	65535	64	1	48	M1460,N,W2,N,N,S	MSS (1460 bytes), NOP, Window Scaling 2, NOP, NOP, Selective ACK OK
WSS = Window Size	MSS = Maximum Segment Size					
TTL = Initial TTL	DF = Don't Fragment Bit					
1. TCP Options and their order						

Рисунок 10.3 – Типичная сигнатура p0f

Этот пример демонстрирует основные принципы пассивного анализа сети. Мы можем использовать аналогичные приемы и методы для описания статистики трафика (процент запросов TCP, UDP, ARP и т.д.), отслеживания состояние соединения, используемой полосы пропускания, числа и размера передаваемых пакетов и т.д.

Потенциальные возможности использования пассивного анализа

Преимущество пассивного анализа заключается в том, что вам не придется ничего делать для сбора данных – они будут собираться во время обычной эксплуатации сети. В конце концов, если бы пользователи и приложения не нуждались в данных на серверах, сети не стояли бы на первом месте. Наши сети постоянно отправляют данные с узлов по всей корпорации, и каждая из этих транзакций является потенциальным источником сбора и анализа данных. Задача нас – аналитиков – состоит в том, чтобы выяснить, какую информацию мы хотим получить из этих данных:

Осведомленность о ситуации

Пассивные методы анализа могут многое сказать нам о нашей сети и о том, как она работает в нормальной ситуации. Без четкого понимания инфраструктуры очень сложно разработать эффективную политику в области безопасности. Например, если вы не знаете адресное пространство, способы доступа в Интернет из сети или операционные системы, установленные в сети, как можно оценить возможность влияния уязвимости и последствия с точки зрения безопасности сети? Или правильно ли размещены у Вас брандмауэры и IDS-датчики в сети?

Политика форсирования.

Пассивный анализ позволяет выявить неразрешенные службы и другие аномальные поведения пользователей в сети практически мгновенно. Простой сбор пакетов с помощью Ethereal или любой другой программы наблюдения за сетью будет определять наличие передачи потоков данных, открытых файлов в Peer-to-peer сетях, игровой активности и другие источники несанкционированного использования сети. Самый простой способ сделать это - использовать Ethereal с фильтром пакетов на определенный IP-адрес внутренней сети, а затем отсортировать по портам TCP или UDP. В большинстве случаев, вы увидите общий набор служб, которые легко идентифицировать, как благоприятные. Эти TCP порты, как правило, используются операционными системами для работы в сети и типичными службами (DNS, FTP, HTTP и т.д.). Главное - это сравнить источники, определенные Вами как авторизованные ресурсы, с полученными в результате пассивного анализа. В конце концов, почему бы Трояну не использовать порт 80 вместо произвольно выбранных эфемерных портов.

Обнаружения утечки инсайдерской информации

Пассивный анализ может помочь выявить уязвимости в системе безопасности, не обнаруженные внутри периметра. Хорошим примером может быть Wualess BackDoor, о котором сообщил Symantec [11, Backdoor.Wualess.C]. Эта угроза открывала BackDoor и пыталась установить связь с IRC-сервером через TCP-порт 5202 в домене dnz.3322.org, используя

канал "# Phantom". Существует три дискретных критерия, по которым мы можем легко определить эту угрозу: присутствие TCP 5202, IRC-протокола в целом и исходящего соединения на этот домен. Если мы осведомлены о ситуации в сети (какие виды трафика разрешается использовать в сети нашего предприятия), то будет легко выявить данную угрозу.

Реакция на инцидент

Пассивный анализ является бесценным инструментом при реагировании на инцидент. Злоумышленники не устанавливают системы, они только их используют. В большинстве случаев исполняемый код злоумышленника работает по тому же принципу. Мониторинг сети в режиме реального времени позволяет определять зону компрометации, какие системы могут быть затронуты нападением и, возможно, как это нападение произошло.

Определения и предупреждения

Эти методы сегодня остаются громоздкими, в основном потому, что практически не существует такой комплексный инструмент, который предоставит весь спектр возможностей пассивного анализа. Тем не менее, они имеют огромный потенциал и легко применимы в большинстве малых и средних сетей с открытым программным обеспечением. Зная наши сети и видя, для чего они используются, мы можем использовать преимущества «игры на своем поле» и перехватить инициативу у злоумышленников.

Данные методы остаются громоздкими, в основном потому, что на рынке представлено не так много комплексного ПО, предоставляющего весь спектр инструментов для пассивного анализа. Тем не менее, они имеют огромный потенциал и легко внедряются в большинство малых и средних сетей с использованием открытого программного обеспечения. Зная, как выглядят наши сети и как они используются, мы можем использовать "преимущество игры на своем поле" и предотвратить нападение на наши системы.

Методические рекомендации по выполнению практического занятия

ПОРЯДОК ВЫПОЛНЕНИЯ

Задания:

1. Разбиться по группам (5 студентов), выполнить групповое задание
2. Сформировать отчет по проделанной работе, на основе скриншотов.
3. Ответить на контрольные вопросы, идущие по ходу выполнения работы (a), b),c)…).
4. Привести примеры методов и средств для пассивного сбора информации о предприятии.

ХОД ВЫПОЛНЕНИЯ РАБОТЫ

Первая фаза тестирования – сбор информации из открытых источников. Reconnaissanc (Recon) переводится, как «разведка». Чем больше информации об организации будет получено, тем больше вероятность успешного проведения тестирования. Один из важнейших аспектов фазы Recon –

произвести инвентаризацию программного обеспечения (ПО) и технической базы. Например, какие в компании используются инструменты для работы с файлами pdf, doc, exl и версии данных программ. Данная информация помогает упростить процесс проникновения внутрь организации (какой использовать эксплоит, какой внедрять вредонос).

Однако, прежде чем преступить к активной фазе изучения организации (выяснение содержимого), проведем предварительный пассивный сбор информации.

Для начала, необходимо изучить специфику организации, терминологию, специфику инфраструктуры, модель типичного сотрудника организации.

Веб-сервис Whois

Далее, посмотрим, что нам даст информация о сайте компании: кем зарегистрирован, какой IP-адрес. Воспользуйтесь сервисом «whois» - либо стандартными средствами Linux (Рисунок 1), либо используя веб-сервисы - www.whois-service.ru (Рисунок 2).

Полученная информация помогает установить место нахождения сайта, либо на сервере организации, либо на арендованном хостинге. Данный факт поможет определить целесообразность анализа веб-приложений организации.

а) Чем ещё может быть полезна информация о домене?

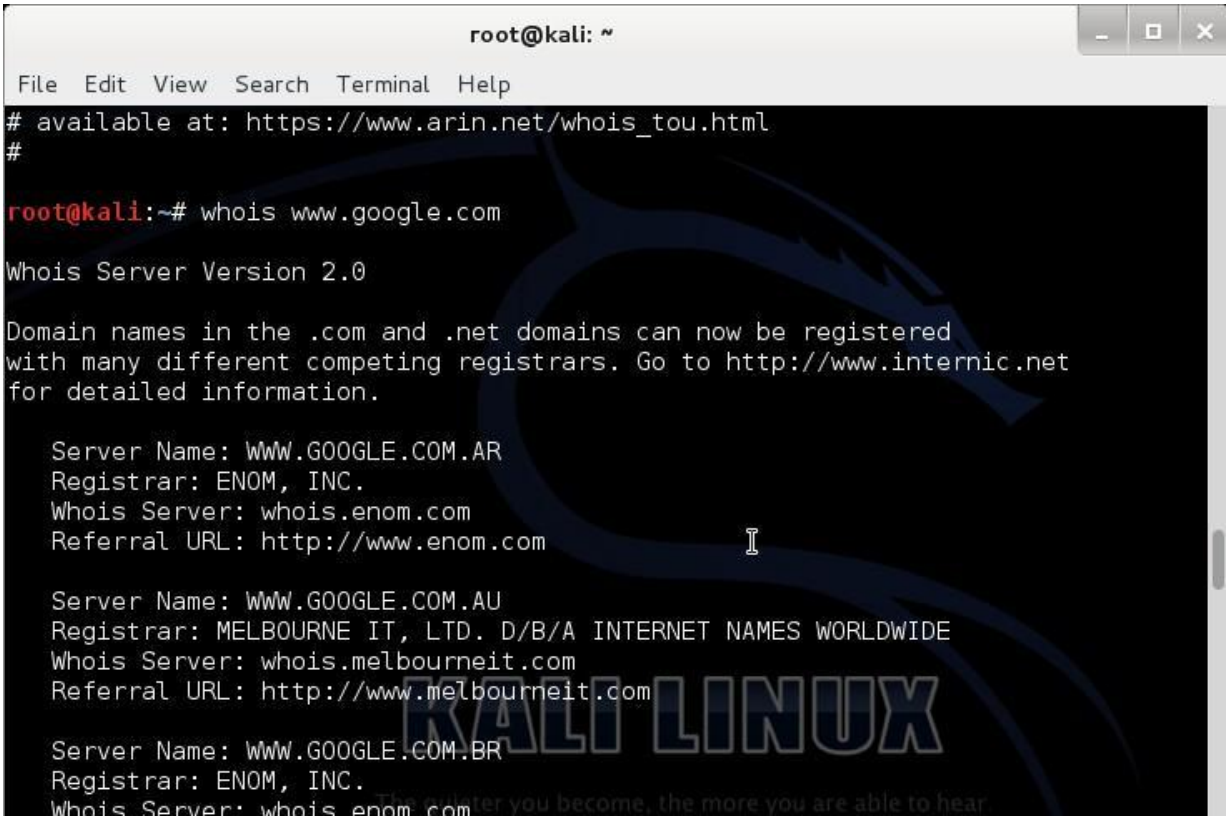


Рисунок 1– Результат работы утилиты «whois»

Рисунок 2 – Веб-интерфейс сервиса «whois»

Поисковый сервис «Google»

1. Следующий полезный инструмент, как ни странно - поисковая система «google».

Google поддерживает использование различных операторов поиска, которые позволяют сузить результаты поисковых запросов.

Попробуйте ввести в поисковую строку ***google URL*** Вашего сайта.

b) Сколько результатов ведал этот поисковый запрос?

А теперь, попробуйте ввести тот же ***URL***, но с использованием оператора site.

c) Какое сейчас количество результатов выдал ***google***?

С помощью оператора ***site*** можно получить все поддомены данного сайта. С этой целью введите в поисковую строку ***google*** запрос по следующему шаблону:

site: example.com – site:www.example.com

d) Какие поддомены организации обнаружил google и сколько?

Так же существуют и другие операторы: ***inurl, intitle, filetype.***

e) Что они означают?

Попробуйте отыскать один из типов файлов (doc, docx, txt, pdf) на сайте, следующим запросом:

site:example.com filetype:pdf

f) Приведите пример работы с другими операторами.

Поиск и извлечение фалов с сайтов – это активная фаза Recon, которой мы займемся в следующей лабораторной работе. Дополню лишь, что фалы нам необходимы для извлечения из них метаданных, с целью узнать о ПО организации.

Утилита «Theharvester»

2. Следующий шаг в изучении – это получение списка личных и корпоративных почтовых адресов сотрудников компании.

Стандартная утилита ***Kali Linux «theharvester»*** позволяет собирать информацию о поддоменах, виртуальных хостах, e-mail адресах, служебных именах (Рисунок 3).

Рисунок 3 – Пример запуска программы «Theharvester»

Попробуйте найти:

theharvester -d example.com -b all

Какие результаты Вы получили? Что значат флаги ***-d, -b.*** Какие еще есть флаги и что они означают?

g) Как Вы думаете, зачем необходима эта процедура?

Утилита «Maltego»

3. Следующий инструмент для получения данных из открытых источников – «Maltego». Это программа, которая может быть использована для выявления отношений и реальных связей между: людьми, группами людей (социальные сети), компаниями, организациями, веб-сайтами, интернет инфраструктурами (доменами, DNS именами, сетевыми блоками, IP адресами, факторами, аффилированности, документами и файлами). Включите «***Maltego***» из бокового меню. Если потребуется вводить данные при входе, то Email: sibsutis.biut@gmail.com, ***Password: test123*** (Рисунок 4).

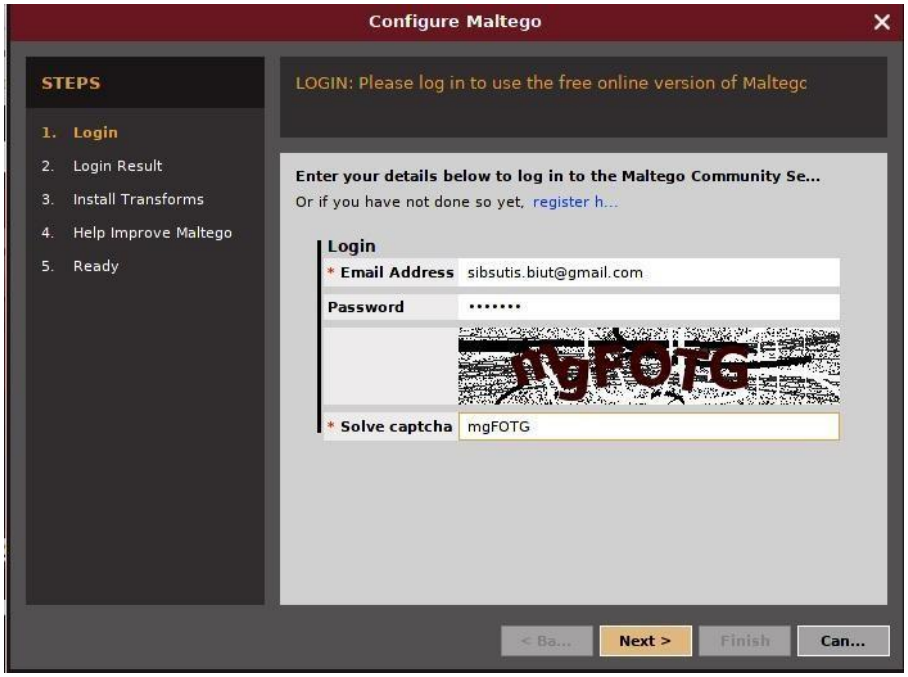


Рисунок 4 - Пример ввода email и пароля

Выберите в левом боковом меню («***EntityPalette***») икону «***Domain***» и перенесите на рабочее поле. Далее, введите адрес Вашего сайта в икону «Domain» и нажмите на нее правой кнопкой мыши. Во всплывшем окне последовательно нажмите на пункты «***Files and Documents***…», «***Email addresses from Domain***», «***All transforms***» (Рисунок 5).

a) Какие, на Ваш взгляд, элементы можно убрать из рабочего поля, после выполнения всех трансформаций?

b) Есть ли разница, между количеством найденных ***E-mail«Maltego»*** и «***Theharvester***»?

c) Какие типы документов удалось получить, используя «***Maltego***»?

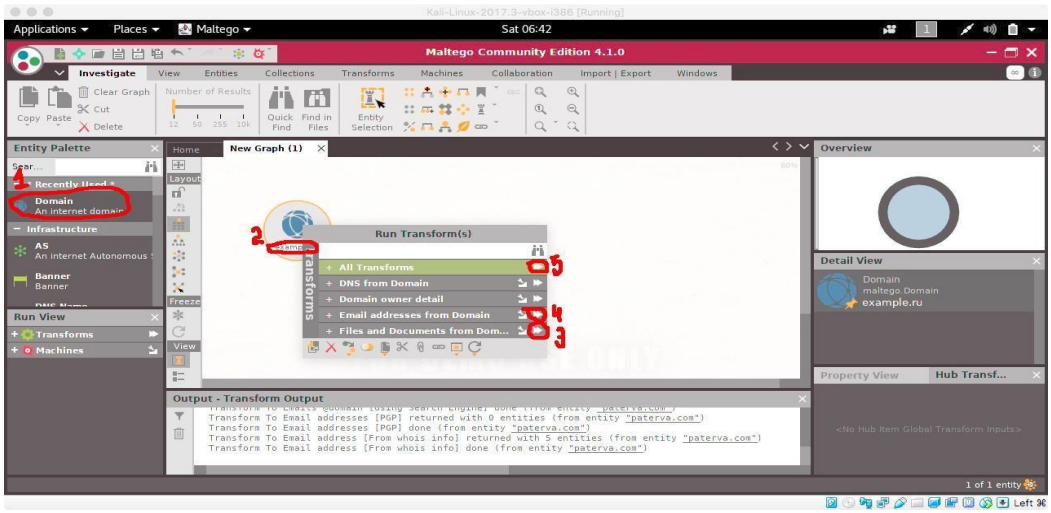


Рисунок 5 - Определение положения необходимых элементов программы

Содержание отчета о практическом занятии

В отчете следует указать:

1. Цель работы;
2. Результат выполнение индивидуального задания;
3. Ответы на контрольные вопросы;
4. Выводы по проделанной работе.
5. Библиография

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ВЫПОЛНЕНИЕ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ

1. www.salut.ru
2. full-steam.ru
3. park-trade.ru
4. teks-trade.ru
5. kailas33.ru
6. ritualflowers.ru
7. sibselmash.nsk.ru
8. b-telecom.ru
9. secourisme.info
10. freescience.info
11. hitgames.net.ua
12. effective.net.ua
13. odarchuk.com
14. gamecheats.net.ru
15. soldatiki.su
16. www.uslugi-moscow.ru
17. www.sbrus.ru
18. .peterburgbanks.ru
19. .mstinfo.ru
20. .mirtour.ru
21. .www.officefile.ru
22. .www.kyznica.ru 2
23. ebs-today.ru
24. vertebrology.ru

Практическая работа № 11

Тема. Правовое регулирование деятельности по защите информации

Цель занятия: Ознакомиться с существующим программным обеспечением для активного сбора информации об организации, получение практических навыков в активном сборе информации, анализ существующих методов и средств активного сбора информации.

Теоретическая часть:

OSINT — разведка и сбор информации из открытых источников

OSINT (англ. Open source intelligence) или разведка на основе открытых источников включает в себя поиск, сбор и анализ информации, полученной из общедоступных источников. Ключевой целью является поиск информации, которая представляет ценность для злоумышленника либо конкурента. Сбор информации во многом является ключевым элементом проведения пентеста. От того, насколько качественно он был осуществлён, может зависеть, как эффективность пентеста в целом, так и эффективность отработки отдельных векторов атаки (социальная инженерия, брутфорс, атака на Web-приложения и пр.). В разрезе кибербезопасности/пентеста OSINT чаще всего применяется для сбора публичных данных о компании, и это касается не только информации о email-адресах ее сотрудников. Не менее интересной будет информация о:

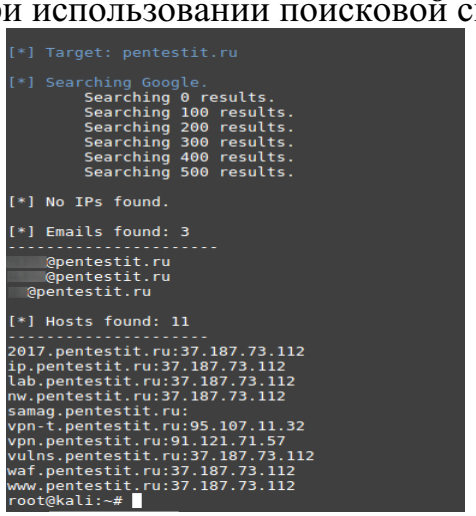
- DNS-именах и IP-адресах;
- доменах и субдоменах, зарегистрированных за компанией;
- фактах компрометации почтовых адресов;
- открытых портах и сервисах на них;
- публичных эксплойтах для найденных сервисов;
- конфиденциальных документах;
- имеющихся механизмах безопасности и т.д.

Сегодня посмотрим с помощью каких инструментов и какую информацию можно найти в открытых источниках.

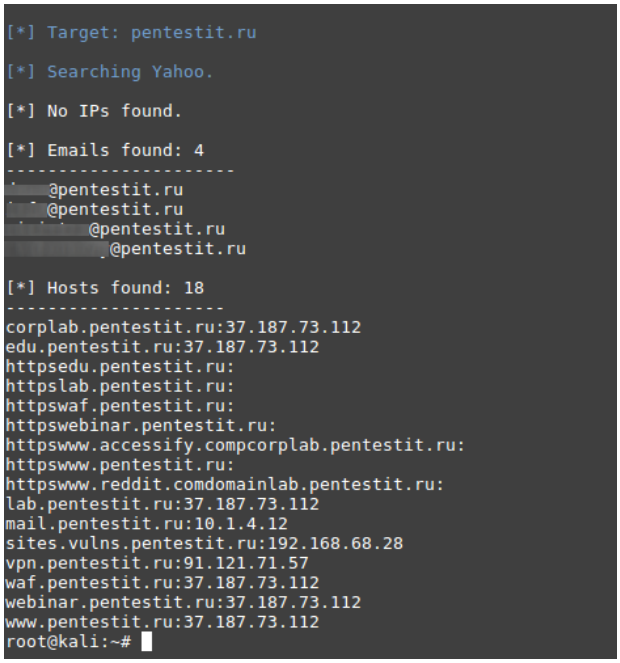
Консольные инструменты

TheHarvester - это целый фреймворк для сбора e-mail адресов, имён субдоменов, виртуальных хостов, открытых портов/банеров и имён сотрудников компании из различных открытых источников. Позволяет производить как пассивный поиск по нескольким поисковым системам: google, yahoo, bing, shodan.io, googleplus, linkedin и т.д., так и активный — например, перебор имен субдоменов по словарю.

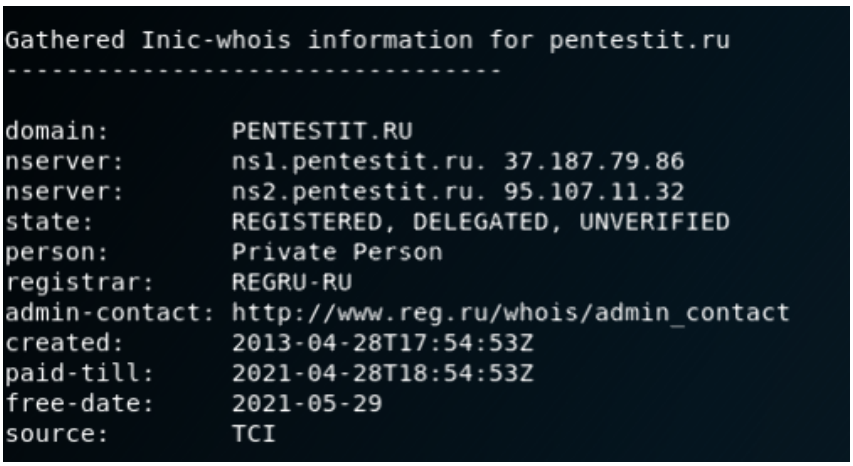
Используя различные поисковые источники можно получить различный результат. Например, при использовании поисковой системы Yahoo:



А при использовании Google:



Dmitry - еще один консольный инструмент для поиска информации об интересующих хостах. Базовый функционал может собирать возможные субдомены, адреса электронной почты, информацию о времени безотказной работы, сканирование TCP-портов, поиск whois и многое другое. Функционал довольно обширный, но по возможностям и скорости обнаружения открытых портов все же уступает предыдущему инструменту, но это не мешает использовать их совместно. Все-таки, подобные вопросы требуют использования информации из разных источников для большей достоверности.



Чтобы получить максимальное количество информации о домене указываем все ключи. В числе прочего, инструмент будет сканировать порты, но в ограниченном диапазоне, поэтому лучше для этих целей использовать Nmap

Nmap («Network Mapper») — это утилита с открытым исходным кодом для исследования сети и проверки безопасности. Она была разработана для быстрого сканирования больших сетей, хотя прекрасно справляется и с единичными целями. Это нестареющая классика и первый инструмент, который используют при проведении пентеста. Его функционал довольно обширен, но в нашем случае от него потребуется только определение открытых портов, названия запущенных сервисов и их версии

```
Not shown: 997 filtered ports
PORT     STATE  SERVICE   VERSION
80/tcp   open   http      nginx
443/tcp  open   ssl/http  nginx
8443/tcp closed https-alt
```

Узнав открытые порты запустим тот же Nmap, но уже будем использовать различные группы скриптов, которые помогут обнаружить возможные ошибки конфигурации:

```
# nmap -sV pentestit.ru --script "version, discovery, vuln, auth" -p22,80,443 –Pn
```

При выполнении этой команды Nmap выполнит все скрипты, собранные в этих группах для получения информации из каждой группы: получение расширенного вывода версии сервисов, поиск расширенной информации о сервере, поиск публичных уязвимостей и т.д. Эта информация так же поможет определить возможные точки входа в сетевой периметр организации.

SpiderFoot - это инструмент автоматизации проведения OSINT. Он интегрируется со многими доступными источниками данных и использует ряд методов анализа данных, что упрощает навигацию по этим данным. SpiderFoot не совсем консольный инструмент т.к. имеет встроенный веб-сервер с интуитивно понятным веб-интерфейсом. Позволяет собирать информацию о:

- IP-адресах;
- Домены/Субдомены;
- Имена пользователей;
- Телефонные адреса;
- Проверка некоторых данных на предмет утечки и т.д.

Google Dork Queries (GDQ) - это набор запросов для выявления индексируемых поисковой системой страниц. Одним словом - всего, что должным образом не спрятано от поисковых роботов. Вот небольшой список команд, которые чаще всего используются:

- **site** - искать по конкретному сайту;
- **inurl** - указать на то, что искомые слова должны быть частью адреса страницы/сайта;
- **intitle** - оператор поиска в заголовке самой страницы;
- **ext** или **filetype** - поиск файлов конкретного типа по расширению.

Комбинируя различным образом команды для поиска можно найти практически все, вплоть до логина/пароля администратора.

Методические рекомендации по выполнению практического занятия

ПОРЯДОК ВЫПОЛНЕНИЯ

Задания:

1. Разбиться по группам (5 студентов), выполнить групповое задание
2. Сформировать отчет по проделанной работе, на основе скриншотов.
3. Ответить на контрольные вопросы, идущие по ходу выполнения работы (a), b),c)…).
4. Привести примеры методов и средств для пассивного сбора информации о предприятии.

ХОД ВЫПОЛНЕНИЯ РАБОТЫ

Процесс активного сбора информации - это, в основном, извлечение метаданных из различных файлов, созданных внутри организации. По этим данным можно определить версию используемого ПО для создания файла, имена и логины сотрудников организации и т.д. Получить такие файлы возможно несколькими способами: от персонала, при проведении им различных тестов; запросить по e-mail; во время тестирования компании из файлового сервера; при помощи web-пауков (web-spider). В рамках лабораторной работы рассмотрим последний вариант получения файлов организации – web-паук.

В Kali-linux существует утилита, позволяющая скачивать файлы по из URLиз командной строки - wget. Однако, это не единственный функционал. Она так же имеет возможность работать как web-паук, рекурсивно скачивая определѐнные типы файлов из указанного домена.

ВНИМАНИЕ!!! Во многих странах применение web-пауков рассматривается как сетевая атака. Организации все вариантов предупреждены о возможных действий студентов. Однако старайтесь не злоупотреблять использованием web-пауков.

Итак, для запуска web-паука с целью получения файлов организации необходимо ввести команду wget со следующими параметрами:

`wget -nd -r -A pdf,doc,docx,xls,xlsx-P <target_directory><target_url>`,

где *<target_directory>* - это директория, куда будут сохранены все найденные файлы; <target_url> - это сайт организации, о которой необходимо собрать информацию (Рисунок 1).

a) Напишите что значат остальные флаги в команде wget.

b) Сколько времени работал web-паук? Сколько файлов было найдено? Приведите вывод в терминале по завершению работы web-паука.

c) Какие ещѐ типы файлов целесообразно рассмотреть?

d) Почему файлы html, php, cgi, asp не целесообразно рассматривать?

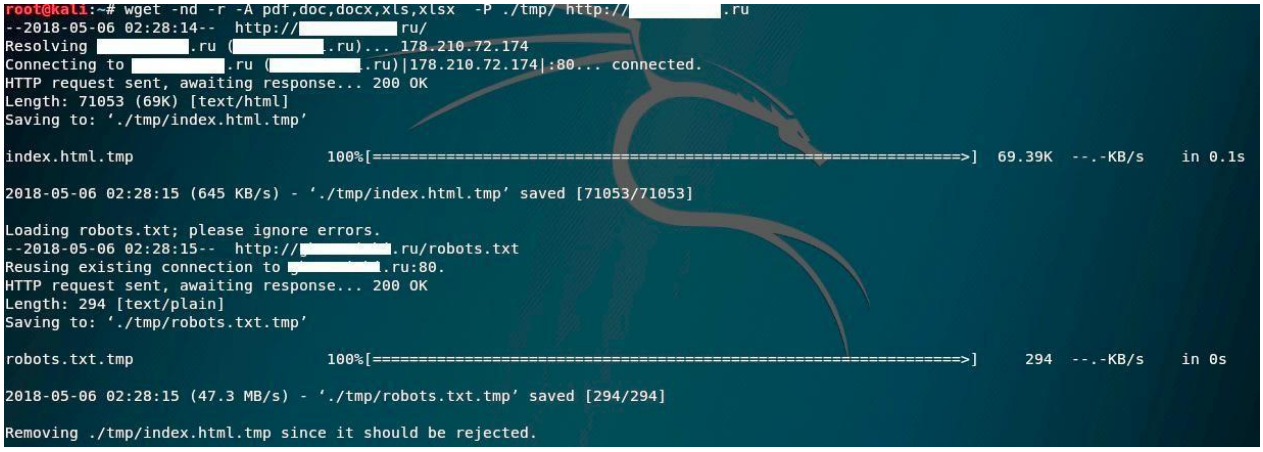


Рисунок 1 - Пример работы web-паука

После получения файлов необходимо изъять из них информацию. Для этого прибегнем к использованию стандартных утилит Kali-linux: Strings, ExifTool (Если в Вашей версии Kali-linuxнет утилиты exiftool, введите в консоли команду `apt-getinstallexiftool--fix-missing` или проследуйте инструкции в Приложение 1).

e) Приведите примеры других программ (на Windows и/или Linux), работающих с метаданными.

f) Какими ещѐ функциями, помимо чтения метаданных, обладает exiftool?

Для получения информации при помощи exiftool, введите в консоли: `exiftool<path_to_file>` (Рисунок 2), где <path_to_file> - это путь к рассматриваемому файлу.

g) Из полученных от web-паука файлов выберите 3 с различными типами и попробуйте достать из них информацию.

h) Какой из типов файлов более информативен, какой менее информативен?

Какие изъятые данные могут быть Вам полезны? Для получения данных из файла утилитой strings, введите в консоли:`strings<path_to_file>` (Рисунок 3), где <path_to_file> - это путь к рассматриваемому файлу.

i) Из полученных от web-паука файлов выберите 3 с различными типами и попробуйте достать из них информацию. Какая полезная информация была изъята при помощи утилиты strings?

j) Сумели ли Вы найти название и версию программы, которой был создан рассматриваемый файл? Если да, приведите пример.

k) Какие существуют аналоги утилиты strings?

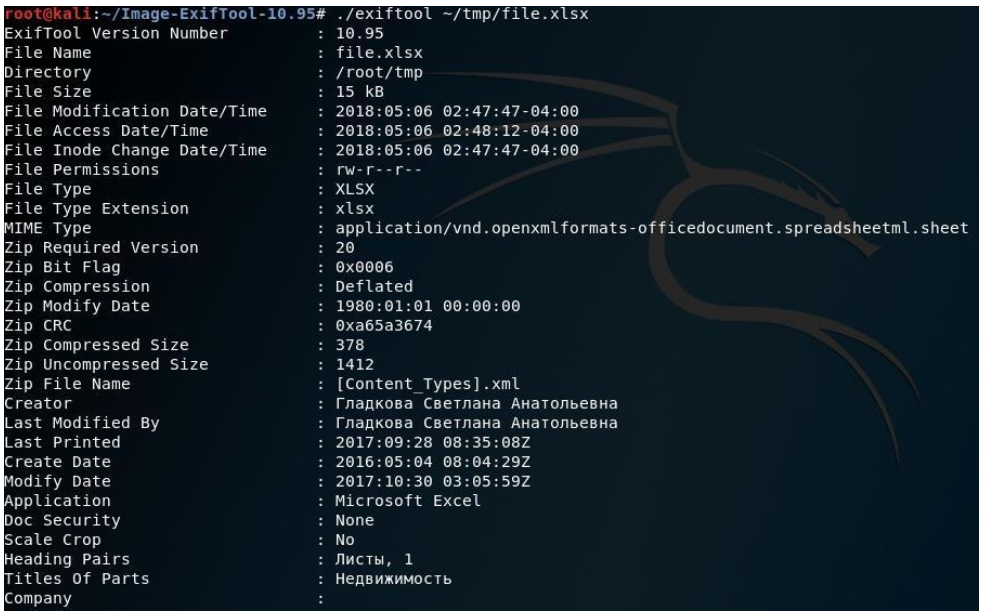


Рисунок 2 - Пример работы утилиты exiftool

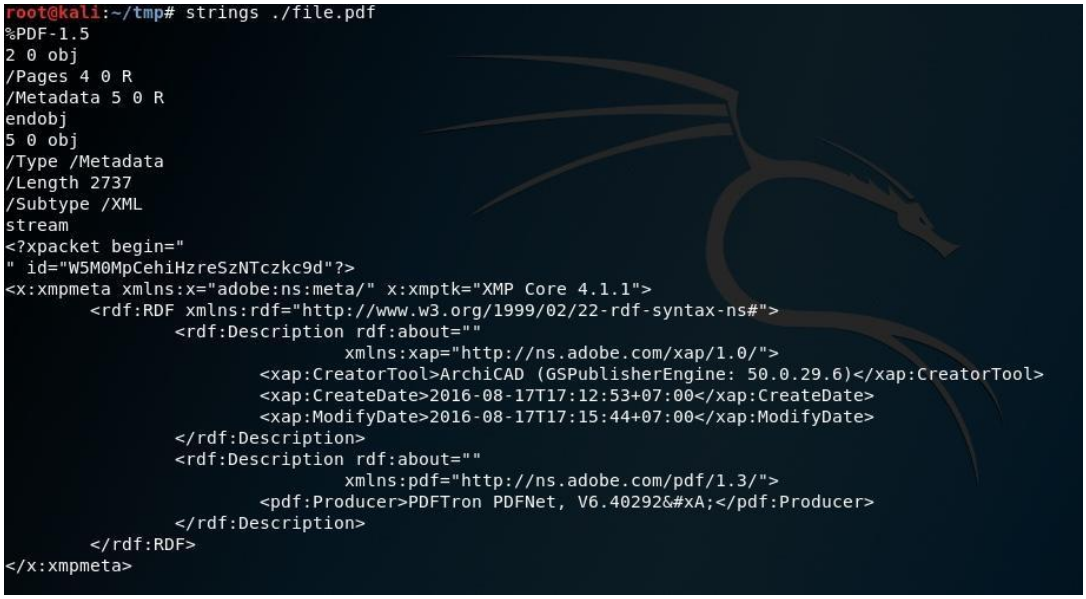


Рисунок 3 - Пример изъятия версии программы, в которой был создан файл, утилитой strings

Содержание отчета о практическом занятии

В отчете следует указать:

1. Цель работы
2. Ход выполнения работы (скриншоты)
3. Выводы по работе

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ВЫПОЛНЕНИЕ ГРУППОВОГО ЗАДАНИЯ

1. www.salut.ru

2. full-steam.ru
3. park-trade.ru
4. teks-trade.ru
5. kailas33.ru
6. ritualflowers.ru
7. sibselmash.nsk.ru
8. b-telecom.ru
9. secourisme.info
10. freescience.info
11. hitgames.net.ua
12. effective.net.ua
13. odarchuk.com
14. gamecheats.net.ru
15. soldatiki.su
16. www.uslugi-moscow.ru
17. www.sbrus.ru
18. .peterburgbanks.ru
19. .mstinfo.ru
20. .mirtour.ru
21. .www.officefile.ru
22. .www.kyznica.ru 2
23. ebs-today.ru
24. vertebrology.ru

Практическая работа № 12

Тема. Нарушения правового характера в сфере информационной безопасности

Цель занятия: Ознакомиться с функциональными возможностями программы nmap, получения навыков работы с программой nmap, ознакомиться с методами сканирования сети и хостов. Получение навыков работы с базой данных уязвимостей CVE.

Теоретическая часть:

Сканирование диапазона IP-адресов

Фундаментальная задача при исследовании любой сети — это сократить набор IP-диапазонов до списка активных хостов. Сканирование каждого порта каждого IP адреса медленно и необязательно. Интерес к исследованию определенных хостов во многом определяется целями сканирования. Задачи администраторов по обнаружению работающих хостов в сети могут быть удовлетворены обычным ICMP-пингом, людям же, которые тестируют способность сети противостоять атакам извне, необходимо использовать разнообразные наборы запросов с целью обхода брандмауэра.

Задачу обнаружения хостов иногда называют пинг сканированием (ping scan), однако она намного превосходит использование обычных ICMP запросов ассоциирующихся с вездесущими ping утилитами. Сканировать сеть предпочтительно с помощью произвольных комбинаций мультипортовых

TCP SYN/ACK, UDP и ICMP запросов. Целью всех этих запросов является получение ответов, указывающих, что IP адрес в настоящее время активен (используется хостом или сетевым устройством). В большинстве сетей лишь небольшой процент IP адресов активен в любой момент времени. Это особенно характерно для адресных пространств вида 10.0.0.0/8. Такие сети имеют 16 млн. IP адресов, но бывают случаи, когда они используются компаниями, в которых не более тысячи машин. Функция обнаружения хостов может найти эти машины в этом необъятном море IP адресов.

Сканирование портов

Существует множество различных приемов сканирования портов и выбираются для конкретной задачи подходящий (или комбинацию из нескольких). Рассмотрим наиболее популярные приемы сканирования:

TCP SYN сканирование SYN это используемый по умолчанию и наиболее популярный тип сканирования. Он может быть быстро запущен, он способен сканировать тысячи портов в секунду при быстром соединении, его работе не препятствуют ограничивающие бренмауэры.

Различные типы UDP сканированияВ то время как большинство сервисов Интернета используют TCP протокол,UDP службы также широко распространены. Тремя наиболее популярными являются DNS, SNMP и DHCP (используют порты 53, 161/162 и 67/68). Т.к. UDP сканирование в общем случае медленнее и сложнее TCP, то многие специалисты по безопасности игнорируют эти порты. Это является ошибкой, т.к. существуют UDP службы, которые используются атакующими.

TCP NULL, FIN и Xmas сканирования. Эти три типа сканирования используют незаметную лазейку в TCP RFC, чтобы разделять порты на открытые и закрытые.

TCP ACK сканирование. Этот тип сканирования сильно отличается от всех других тем, что он не способен определить открый порт. Он используются для выявления правил брандмауэров, определения учитывают ли он состояние или нет, а также для определения фильтруемых ими портов.

Обнаружение служб и их версий

При сканировании удаленной системы может быть выявлено, что порты25/tcp,80/tcp, и 53/udp открыты. Используя сведения можно узнать, что эти порты, вероятно, соответствуют почтовому серверу (SMTP), веб-серверу (HTTP), и серверу доменных имен (DNS) соответственно. Эта информация обычно верна, т.к. подавляющее большинство служб, использующих 25 TCP порт, фактически, почтовые сервера. Тем не менее, не следует полностью полагаться на эту информацию. Люди могут и запускают службы с использованием нестандартных портов.

После обнаружения каких-либо TCP и/или UDP портов происходит процедура их идентификации с целью определения приложений (службы) их использующих. Используя базу данных запросов для обращения к различным службам и соответствующие выражения для распознавания и анализа ответов можно определить протоколы службы (напр. FTP, SSH,

Telnet, HTTP), имя приложения (e.g. ISC BIND, Apache httpd, Solaris telnetd), номер версии, имя хоста, тип устройства (напр. принтер, роутер), семейство ОС (напр. Windows, Linux) и иногда различные детали типа: возможно ли соединится с X сервером, версию протокола SSH, или имя пользователя.

Сканирование для определения ОС

Возможно, определить ОС на удаленной системе на основе анализа работы стека TCP/IP. Посылается серия TCP и UDP пакетов на удаленный хост и изучается практически каждый бит в ответах. После проведения множества тестов, таких как TCP ISN выборки, поддержки опций TCP, IP ID выборки, и анализа продолжительности процедуры инициализации, сравнивается результаты с базой данных, содержащей известные наборытипичных результатов для различных ОС и, при нахождении соответствий, можно сделать вывод об установленной ОС.

Сканирование уязвимостей

Сканирование уязвимостей — полностью или частично автоматизированный процесс сбора информации о доступности сетевого узла информационной сети (персональные компьютеры, серверы, телекоммуникационное оборудование), сетевых службах и приложениях используемых на данном узле и их идентификации, используемых данными службами и приложениями портах, с целью определения существующих или возможных уязвимостей.

Методические рекомендации по выполнению практического занятия

ПОРЯДОК ВЫПОЛНЕНИЯ

Задания:

1. Разбиться по группам (5 студентов), выполнить групповое задание
2. Сформировать отчет по проделанной работе, на основе скриншотов.
3. Ответить на контрольные вопросы, идущие по ходу выполнения работы (a), b),c)…).
4. привести примеры методов и средств для пассивного сбора информации о предприятии.

ХОД ВЫПОЛНЕНИЯ РАБОТЫ

Следующим этапом, после сбора информации о компании – это сканирование. Сканирование может быть разным, в зависимости от поставленной задачи и условий. Если Вы имеете доступ к внутренней сети организации, то, как было сказано выше, производится идентификация объектов внутри сети и выбирается интересующие объекты, для более детального сканирования. Так же, может стоять задача проникновения внутрь сети. Тогда, в большинстве случаев, Вам предоставят «белый» IP- адрес сервера/шлюза компании. Суть такой задачи – найти уязвимости или ошибки конфигурации на устройстве и попытаться проэксплуатировать их.

Выполнять сканирование предлагается утилитой nmap.

Nmap умеет сканировать различными методами — например, UDP, TCP connect(), TCP SYN (полуоткрытое), FTP proxy (прорыв через ftp), Reverse-ident, ICMP (ping), FIN, ACK, SYN и NULL-сканирование. Выбор варианта сканирования зависит от указанных ключей, вызов nmap выглядит следующим образом:

nmap <ключи> цель

Nmap распознаѐт следующие состояния портов: **open**, **filtered**, **closed**, или **unfiltered**. «Open» означает, что приложение на целевой машине готово для принятия пакетов на этот порт. Filtered означает, что брандмауэр, фильтр, или что-то другое в сети блокирует порт, так что Nmap не может определить, является ли порт открытым или закрытым. Closed — не связанны в данный момент ни с каким приложением, но могут быть открыты в любой момент. Unfiltered порты отвечают на запросы Nmap, но нельзя определить, являются ли они открытыми или закрытыми.

В данной работе рассмотрим сканирование nmap'ом одного хоста. Начнем с небольшого изучения полезных опций. Первая опция «--packet-trace» включает режим дебага (Debug). Это значит, что Вы можете видеть какие пакеты и куда отправляются, статус соединения, ответ от соседа. Для последующего отключения/включения данного режима нажмите SHIFT-p. Для смены режима дебага – SHIFT-v.

a) Продемонстрируйте работу nmap в режиме «--packet-trace».

Следующая опция времени «-T». Всего существует 6 опций времени. Рассмотрим 2 крайности: «-T0» - опция времени, которая позволяет работать сканеру очень медленно, чтобы не быть замеченным IDS системами; «-T4» - это агрессивный тип сканирования, который распараллеливает процесс сканирования, и отводит не более 1.25 на ожидание ответа.

b) Приведите примеры остальных опций и их предназначение.

c) Продемонстрируйте время работы опций «-T0», «-T4». (Запускайте «-T0» в конце проведения работы, так как результат может быть более 1 часа).

Так же, nmap владеет методами централизованной записи результатов сканирования в разные форматы. Чаще всего, используют флаги «-oN», «-oA»для записи в файл выходной информации, понятной человеку.

d) Приведите примеры других опций записи результатов в файл и их значение.

Опция «-p» отвечает за перечисление сетевых портов, которые необходимо просканировать. По умолчанию, nmap сканирует первые 1000 портов. Однако, не во всех случаях этого достаточно. После «-p» можно перечислять порты через запятую и/или указывать диапазон значений портов. Для запуска сканирования по всем портам, используют значение «-p 1-65535».

Очередная полезная опция - «-n». Она отключает разыменование доменных имен.

Опция «-O» позволит Вам определить версию операционной системы.

Так же, существует опция «-A», которая отвечает за агрессивное сканирование в целом. В еѐ состав входят опции «-sV», «-sC», «-O», «--

traceroute». «-sV» - этот флаг позволяет определить программу на хосте, которая открыла данных порт, и еѐ версию; «--traceroute» - определяет количество роутеров от Вас до исследуемого хоста.

e) За что отвечает опция «-sC».

f) Запустите nmap в агрессивном режиме сканирования, сканируя все порты, без разыменования доменных имен, сохранив результат в понятном виде.

g) Ознакомьтесь с понятием CVE и базой уязвимостей (https://xakep.ru/2009/05/15/48221/).

h) Ознакомьтесь со стадиями присвоения уникального номера уязвимости (https://xakep.ru/2009/05/15/48221/).

i) Используя результат из пункта «F» и «Приложение 1», заполните «Таблицу 1».

Таблица 1 – Форма представления результатов выполнения работы

N	Ресурс	Уязвимый сервис	Код CVE	Рейтинг CVE	Тип уязвимости	Порт сервиса	Уязвимый параметр	Варианты закрытия уязвимости
1								

Содержание отчета о практическом занятии

В отчете следует указать:

1. Цель работы
2. Ход выполнения работы (скриншоты)
3. Выводы по работе

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ВЫПОЛНЕНИЕ ГРУППОВЫХ ЗАДАНИЯ

1. http://www.dsm.com
2. http://www.schools.nsw.edu.au
3. http://thetablet.co.uk
4. http://www.scstatehouse.gov
5. http://www.highered.tafensw.edu.au
6. http://www.mcdonalds.com
7. http://www.watersportholland.nl
8. http://www.watersportholland.nl
9. http://www.networkcomputing.com
10. http://www.unc.edu
11. http://cugir.mannlib.cornell.edu
12. http://ieeexplore.ieee.org
13. http://vivo-is.cns.iu.edu
14. http://google.nyu.edu
15. http://ofa.fas.harvard.edu

16. http://www.uidaho.edu
17. https://vivo.ufl.edu
18. http://energy.gov

Практическая работа № 13

Тема. Правовые основы и особенности расследования преступлений в сфере информационной безопасности

Цель занятия: Изучение основ правового регулирования общественных отношений в области конфиденциальной информации.

Теоретическая часть:

Информация ограниченного доступа, включающая государственную тайну и конфиденциальную информацию, имеет особую важность для государства и общества. В той или иной мере правовые институты тайн есть во всех развитых демократиях мира.

Опыт показывает, что с ростом значимости информации в общей системе государственного и муниципального управления (ГМУ) наиболее важным элементом с годами становится достижение превосходства в информационной сфере. Этим обстоятельством и определяется существование институтов тайн, создающих возможность для ГМУ проводить независимую информационную политику, защищать свои интересы, осуществлять управление обществом, регионом, муниципальным образованием.

Система секретной и конфиденциальной информации – наиболее сильное звено регулирования общественных отношений в информационной сфере. Вследствие возможного существенного ущерба от ее разглашения информация ограниченного доступа занимает особое место в системе управления. Институт тайн – важнейший элемент системы государственного и муниципального управления.

Основу нормативно-правового обеспечения защиты информации ограниченного доступа в России составляют Конституция РФ, законы «О безопасности» от 5 марта 1992 года № 2446-1, «О государственной тайне» от 21 июля 1993 года № 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ и другие.

В условиях сегодняшней России (расширяющееся международное сотрудничество, либерализация экономики, увеличение количества объектов иностранных инспекций, свободное перемещение иностранцев по большей части территории страны, внедрение компьютерной техники иностранного производства) значительной возросла опасность утечки сведений, составляющих информацию ограниченного доступа. Вследствие этого важнейшими задачами органов ГМУ являются обеспечение необходимого баланса между потребностью в свободном обмене информацией и допустимыми ограничениями на ее распространение, а также развитие и защита государственного и муниципального ресурса.

В действующем законодательстве РФ встречается упоминание более чем о 30 видах различных тайн (государственная, служебная, коммерческая, банковская, личная, семейная, тайна следствия, связи, почтовых отправлений и другие).

Приведем наиболее важные определения в этой области и дадим необходимую классификацию.

Защищаемой информацией называется информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации.

Собственником информации может быть государство, юридическое лицо, группа физических лиц, отдельное физическое лицо. К защищаемой информации относится информация с ограниченным доступом, а также открытая информация, представляющая ценность.

Информацией с ограниченным доступом называется информация, доступ к которой ограничен в соответствии с Законом с целью защиты прав и законных интересов субъектов права на тайну. Она состоит из государственной тайны и конфиденциальной информации.

Конфиденциальная информация в свою очередь включает множество видов тайны, которые сводятся к шести основным видам:

1) персональные данные;
2) тайна следствия и судопроизводства;
3) служебная тайна;
4) профессиональная тайна;
5) коммерческая тайна;
6) тайна изобретения, полезной модели и промышленного образца.

Особую важность с точки зрения безопасности государства имеет защита информации, составляющей государственную и служебную тайну.

Государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Конфиденциальная информация – информация, не составляющая государственную тайну, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Персональные данные – сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях.

Тайна следствия и судопроизводства – защищаемая по закону конфиденциальная информация, ставшая известной в органах следствия и судопроизводства только на законных основаниях в ходе следствия и судопроизводства, а также служебная информация о деятельности органов

следствия и судопроизводства, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Служебная тайна – защищаемая по закону конфиденциальная информация, ставшая известной в государственных органах и органах местного самоуправления только на законных основаниях и в силу исполнения их представителями служебных обязанностей, а также служебная информация о деятельности государственных органов, доступ к которой ограничен федеральным законом или в силу служебной необходимости.

Профессиональная тайна – сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией РФ и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений, банковская тайна и т. д.).

Коммерческая тайна – научно-техническая, технологическая, коммерческая, организационная или иная используемая в экономической деятельности информация, имеющая действительную потенциальную коммерческую ценность в силу ее неизвестности третьим лицам, к которой нет свободного доступа на законном основании и по отношению к которой принимаются адекватные ее ценности меры охраны.

Тайна изобретения, полезной модели или промышленного образца – сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них.

Согласно законодательству, обязательными признаками информации с ограниченным доступом должны быть:

1. Информация имеет действительную или потенциальную ценность для ее обладателя в силу неизвестности ее третьим лицам. Такими лицами могут быть государство, юридические или физические лица.

2. К информации нет свободного доступа на законном основании. Возможность сохранения ее неизвестной для третьих лиц установлена законом.

3. Обладатель информации принимает меры по ее защите.

К государственной тайне относятся сведения, удовлетворяющие следующим признакам:

1. Сведения в строго установленных сферах деятельности государства (военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно розыскной деятельности) и ни в каких других.

2. Сведения, не известные широкому, точнее – неопределенному неконтролируемому кругу лиц, и представляющие ценность именно в силу такой неизвестности.

3. Сведения, распространение которых может нанести ущерб безопасности РФ. При этом величина ущерба такова, что влияет на безопасность государства.

4. Сведения, относительно которых предпринимаются специальные меры защиты, направленные на предотвращение их неконтролируемого распространения.

Система документов по защите государственной тайны

Документы по защите государственной тайны по функционально-целевому назначению подразделяются на следующие основные классы:

- нормативные правовые;
- организационно-распорядительные;
- нормативные;
- плановые;
- информационные.

Нормативные правовые акты в области защиты государственной тайны включают:

- федеральные законы;
- указы и распоряжения Президента РФ;
- постановления и распоряжения высших органов исполнительной и судебной властей РФ.

Базовыми законами в области защиты государственной тайны являются специальные законы «О государственной тайне» от 21 июля 1993 года

№ 5485-1, «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 года № 149-ФЗ, а также нормативные правовые акты более общего характера: Конституция РФ, Гражданский и Уголовный кодексы РФ и др.

На их основе организационно-распорядительные документы определяют состав и регламентируют деятельность соответствующих органов и служб при организации и осуществлении защиты государственной тайны. Эти документы по характеру регламентируемых вопросов (решаемых задач) и продолжительности действия подразделяют на два вида:

- основополагающие (руководящие) документы;
- распорядительные документы (документы оперативного управления).

Основополагающие (руководящие) документы помимо самостоятельного использования служат основой при разработке нормативных, плановых и информационных документов. Они являются подзаконными актами, детализирующими и раскрывающими положения нормативных правовых актов, и устанавливают основные направления, единые принципы, порядок организации защиты государственной тайны соответствующими органами и службами с приведением их задач, функций, прав, обязанностей и мер ответственности.

Положения по защите государственной тайны издаются на основе нормативных правовых актов и принятых концепций и детализируют указные документы, в основном по вопросам организации защиты государственной тайны в конкретном органе государственной власти (ведомстве) и, в частности, регламентируют:

- основные направления работ по защите государственной тайны;

− структуру органов и служб, ответственных за организацию и осуществление защиты государственной тайны, их права и обязанности;

− порядок организации и проведения типовых работ по защите государственной тайны для основных объектов защиты;

− финансово-экономические вопросы обеспечения работ по защите государственной тайны;

− вопросы государственного лицензирования в области защиты государственной тайны.

Детальные разъяснения отдельных практических вопросов по организации и осуществлению защиты государственной тайны включаются в соответствующие руководства, наставления, инструкции и правила.

Распорядительные документы – документы текущего (оперативного) управления издают во исполнение или в дополнение к основополагающим документам. Основными видами распорядительных документов по защите государственной тайны являются решения, приказы, директивы, распоряжения, указания.

Нормативные документы устанавливают единые требования, нормы и правила защиты информации, составляющей государственную тайну, обязательные для исполнения в пределах установленной при их введении сферы действия и области их распространения.

Основными видами нормативных документов, в которых регламентируются вопросы защиты государственной тайны, являются:

специальные нормативные документы федеральных органов исполнительной власти, ответственных за обеспечение защиты государственной тайны;

− нормативные документы государственной системы стандартизации.

К специальным нормативным документам относятся:

− требования и нормы по защите государственной тайны;

− методики проведения работ в области защиты государственной тайны;

− лицензии предприятиям на право осуществления работ в области защиты государственной тайны;

− сертификаты соответствия средств защиты информации;

− аттестаты на объекты защиты.

Плановые документы включают целевые программы и планы в области защиты государственной тайны или соответствующие разделы программ и планов более общего характера, по которым осуществляется самостоятельное финансирование.

Информационные документы служат для информационного обеспечения решения задач организации и осуществления защиты государственной тайны.

По форме представления информационные документы могут быть следующих видов:

− справочные документы;

− отчетная научно-техническая документация;

- учебная и научная литература;
- формы документов служебного делопроизводства.

Федеральный закон «О государственной тайне»

Положения федерального закона «О государственной тайне» от 21 июля 1993 года № 5485-1 обязательны для исполнения на территории Российской Федерации и за ее пределами органами законодательной, исполнительной и судебной властей, местного самоуправления, предприятиями, учреждениями и организациями, независимо от их организационно-правовой формы и формы собственности, должностными лицами и гражданами Российской Федерации, взявшими на себя обязательства либо обязанными по своему статусу исполнять требования законодательства Российской Федерации о государственной тайне.

Термины, используемые в законе, их определения

Государственная тайна – защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведыватель-ной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Носители сведений, составляющих государственную тайну – материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов сигналов, технических решений и процессов.

Система защиты государственной тайны – совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

Допуск к государственной тайне – процедура оформления права граждан на доступ к сведениям, составляющим государственную тайну, а также предприятий, учреждений и организаций – на проведение работ с использованием таких сведений.

Доступ к сведениям, составляющим государственную тайну – санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну.

Гриф секретности – реквизиты, свидетельствующие о степени секретности сведений, содержащихся в их носителе, проставляемые на самом носителе и (или) в сопроводительной документации на него.

Средства защиты информации – технические, криптографические, программные и другие средства, предназначенные для защиты сведений, составляющих государственную тайну, средства, в которых они реализованы, а также средства контроля эффективности защиты информации.

Перечень сведений, составляющих государственную тайну, совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Правовой режим защиты государственной тайны

Перечневый подход к организации защиты государственной тайны

В настоящее время в России существуют как открытые, так и закрытые перечни сведений. Открытыми перечнями являются приведенный в Законе «О государственной тайне» перечень сведений, составляющих государственную тайну, а также утверждаемый Указом Президента РФ перечень сведений, отнесенных к государственной тайне. Кроме того, существуют ведомственные перечни сведений, подлежащих засекречиванию, которые могут быть как открытыми, так и закрытыми.

С их помощью реализуется подход к организации защиты государственной тайны в виде системы перечней, включающей:

- перечень сведений, составляющих государственную тайну (определен в Законе «О государственной тайне»);
- перечень сведений, отнесенных к государственной тайне (утверждается Указом Президента РФ);
- развернутый перечень сведений, подлежащих засекречиванию в органе государственной власти (утверждается руководителями органов власти, руководители которых наделены полномочиями по отнесению сведений к государственной тайне);
- перечни сведений, подлежащих засекречиванию, на предприятии, в учреждении и организации (представляют собой выписки из развернутых перечней сведений, подлежащих засекречиванию).

Перечень сведений, составляющих государственную тайну – совокупность категорий сведений, в соответствии с которыми сведения относятся к государственной тайне и засекречиваются на основаниях и в порядке, установленных федеральным законодательством.

Отнесение сведений к государственной тайне осуществляется в соответствии с Перечнем сведений, составляющих государственную тайну, определяемым Законом «О государственной тайне», руководителями органов государственной власти в соответствии с Перечнем должностных лиц, наделяемых полномочиями по отнесению сведений к государственной тайне, утверждаемым Президентом РФ. Указанные лица несут персональную ответственность за принятые ими решения о целесообразности отнесения конкретных сведений к государственной тайне.

Перечень не закрепощает набор конкретных сведений путем прямого отнесения их к государственной тайне, а лишь создает законодательную базу для отнесения конкретных сведений к государственной тайне, если для этого имеется соответствующее обоснование. Такой подход должен позволить системе засекречивания адаптироваться к динамичному развитию нашего общества, ослабить искусственную секретность, наносящую ущерб экономическим интересам РФ.

Установлена персональная ответственность конкретных должностных лиц за принятие решения по отнесению сведений к государственной тайне. Именно за ними сохраняется ответственность за обоснованность, в том числе экономическую, установленной степени секретности конкретных сведений. Именно на них возложена функция гибкого и своевременного реагирования

на внешние условия изменения режима секретности, чтобы последний не превращался в фактор, тормозящий развитие экономики, науки и межгосударственных отношений.

Методические рекомендации по выполнению практического занятия

ПОРЯДОК ВЫПОЛНЕНИЯ

1. Работа выполняется согласно групповому заданию (группы по 5 студентов).

2. П. 2 задания выполняются в таблице.

3. Ссылки на нормативные правовые акты указываются в тексте работы в соответствии с приведенными примерами.

4. Ответы формулируются по существу вопроса. Цитирование положений нормативных правовых актов допускается при условии их полного соответствия заданию.

Содержание отчета о практическом занятии

1. Цель работы.
2. Результат выполнения работы.
3. Выводы.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ВЫПОЛНЕНИЕ ГРУППОВОГО ЗАДАНИЯ

1	Сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность, за исключением сведений, подлежащих распространению в средствах массовой информации в установленных федеральными законами случаях
2	Сведения, составляющие тайну следствия
3	Сведения, о лицах, в отношении которых согласно нормативными правовыми актами Российской Федерации принято решение о применении мер государственной защиты и о мерах государственной защиты указанных лиц
4	Сведения, в сфере управления, доступ к которым ограничен органами государственной власти
5	Сведения, составляющие адвокатскую тайну
6	Сведения, составляющие тайну переписки
7	Сведения, составляющие врачебную тайну
8	Сведения любого характера (производственные, технические, экономические, организационные и другие), которые имеют действительную или потенциальную коммерческую ценность в силу

	неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании
9	Сведения о способах осуществления профессиональной деятельности, которые имеют действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, к которым у третьих лиц нет свободного доступа на законном основании
10	Сведения о сущности изобретения, полезной модели или промышленного образца до официальной публикации информации о них

1. Установить тип сведений согласно индивидуальному заданию.
2. Указать источники права в области оборота сведений согласно индивидуальному заданию.

№	**Название НПА** (согласно юридической силе)	**Указать соответствующие положения НПА**

3. Установить вид(ы) правовых режимов защиты информации, действие которых распространяется на сведения согласно индивидуальному заданию.
4. Указать меры, которые устанавливаются для обеспечения правового режима сведений согласно индивидуальному заданию.
5. Установить правовой статус субъектов в области оборота сведений согласно индивидуальному заданию.
6. Указать основания и меры (вид и размер) юридической ответственности, применяемой к субъектам в области оборота сведений согласно индивидуальному заданию.
7. Если сведения относятся к государственной тайне проанализировать порядок установления степени их секретности.

Практическая работа № 14

Тема. Борьба с компьютерными преступлениями

Цель занятия: Формирование понимания механизмов реализации правовых отношений в области защиты интеллектуальных прав.

Теоретическая часть:

Примеры решения задач

Задача 1

Студент 5-го курса технического ВУЗа Куприянов А. написал в рамках курсовой работы компьютерную программу «TEST», позволяющую проводить тестирование остаточных знаний по ряду математических дисциплин.

Назовите объекты и субъекты авторского права.

Кому принадлежат личные неимущественные и исключительные права на данное программное обеспечение (ПО)?

Решение

Согласно ст. 1259 ГК РФ к объектам авторских прав относятся произведения науки, литературы и искусства, в том числе и программы для

ЭВМ, которые охраняются как литературные произведения. На основании этого объектом авторского права в данном случае является программа «TEST»,

Субъектами авторского права являются:

авторы произведений (ст. 1228 п.1 ГК РФ, ст. 1257 ГК РФ); их наследники (ст. 1267 ГК РФ); другие правопреемники (ст. 1267 ГК РФ), которыми могут быть физическими и юридическими лицами;

Российское государство (ст. 1282 ГК РФ). В данном случае субъектом авторского права является студент Куприянов А. (автор программы).

На основании ст. 1228 п.2 ГК РФ автору результата интеллектуальной деятельности принадлежит право авторства, право на имя и иные личные неимущественные права, следовательно, личные неимущественные права принадлежат автору программы Куприянову А.

Исключительные права на данное ПО принадлежат также Куприянову, т.к. согласно ст. 1228 п.3 исключительное право на результат интеллектуальной деятельности, созданный творческим трудом, первоначально возникает у его автора. Это право может быть передано автором другому лицу по договору, а также может перейти к другим лицам по иным основаниям, установленным законом. В данном случае Куприянов исключительные права на разработанную им программу не передавал.

Задача 2

Индивидуальный предприниматель Жильцов А.А. умер. Он являлся единоличным автором двух программных продуктов «Fox» и «Ling», которые пользовались большим спросом на рынке ПО в области игровых программ. При жизни Жильцов А.А. не передавал права на данные программные продукты, у него нет наследников и он не оставил завещания.

Кому после смерти Жильцова А.А. перейдут личные неимущественные и исключительные права на данные программные продукты?

Каковы сроки действия этих прав на указанное ПО?

Решение

На основании ст. 1228 п.2 право авторства, право на имя и иные личные неимущественные права автора неотчуждаемы и непередаваемы, следовательно, личные неимущественные права остаются за Жильцовым А.А. Согласно ст. 1267 п.1, авторство, имя автора и неприкосновенность произведения охраняются бессрочно.

Т.к. Жильцов А.А. не оставил завещания, то согласно ст. 1283 ГК РФ, исключительное право на программные продукты «Fox» и «Ling» переходит наследникам. На основании ст. 1151 ГК РФ в случае, если отсутствуют наследники как по закону, так и по завещанию, либо никто из наследников не имеет права наследовать или все наследники отстранены от наследования (ст. 1117 ГК РФ), либо никто из наследников не принял наследства, либо все наследники отказались от наследства и при этом никто из них не указал, что отказывается в пользу другого наследника (ст. 1158 ГК РФ), имущество

умершего переходит в порядке наследования по закону в собственность Российской Федерации.

Методические рекомендации по выполнению практического занятия

ПОРЯДОК ВЫПОЛНЕНИЯ

1. Решить задачи в группах по 5 студентов.

2. Ответы на задания, поставленные к задачам, оформите в виде таблицы.

Результаты практического занятия занести в отчет о выполнении практического занятия.

Содержание отчета о практическом занятии

1. Цель работы.

2. Результат выполнения задания в таблице.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ВЫПОЛНЕНИЕ ЗАДАНИЯ

Задача 1

Работник IT управления компании А. в установленном порядке оформил государственную регистрацию права на программу для ЭВМ, созданную в процессе выполнения служебного задания. В суд поступил иск от директора данного управления Б. о включении его в число соавторов, поскольку он осуществлял организацию деятельности по созданию программы и непосредственное руководство работами, вносил предложения и коррективы в создаваемый продукт. Условия реализации права авторства договором не оговорены.

1. Укажите виды интеллектуальных прав на указанную в условии программу.

2. Укажите правосубъектность гражданина А., Б. и соответствующего работодателя в сфере реализации авторских прав на указанную программу.

3. Сформулируйте решение по указанному делу.

4. Сделайте выводы о том, какие действия должны быть предприняты для реализации комплекса авторских прав при условии создания соответствующего объекта.

Решение задачи (оформление ответов)

1	***Виды интеллектуальных прав на программу ЭВМ***	
2	***Правосубъектность гражданина А. (ответчика)***	
3	***Правосубъектность гражданина Б. (истца)***	

4	***Правосубъектность работодателя***	
5	***Решение по указанному делу***	
6	***Выводы о том, какие действия должны быть предприняты для четкой реализации комплекса авторских прав при условии создания соответствующего объекта***	

Задача 2

Гражданин Б. обратился в суд с иском в отношении ряда издательств о защите интеллектуальных прав, а также взыскании компенсации за неправомерное использование его произведений и компенсации морального вреда. Указанные автором издания опубликовали и реализовали сборники, содержащие произведения, которые частично копируют сочинения истца. При этом фрагменты из сочинений истца составляют большую часть текста, положенного в основу произведений, размещенных в сборнике.

Автор посчитал, что ответчики нарушили его интеллектуальные права на созданные им произведения, реализовав сборники, содержащие фрагменты его сочинений.

1. Раскройте сущность основных понятий.
2. Укажите виды неимущественных интеллектуальных прав автора на указанные в условии произведения.
3. Укажите виды имущественных интеллектуальных прав автора на указанные в условии произведения.
4. Назовите особенности правовой защиты личных неимущественных прав.
5. Назовите особенности правовой защиты личных имущественных прав.
6. Назовите уточнения, которые могут потребоваться для решения судебного спора.
7. Сформулируйте возможное решение по указанному делу.

Решение задачи (оформление ответов)

1	***Сущность основных понятий***	
2	***Виды неимущественных интеллектуальных прав автора***	
3	***Виды имущественных интеллектуальных прав автора***	
4	***Особенности правовой защиты личных неимущественных прав***	
5	***Особенности правовой защиты личных имущественных прав***	

6	***Уточнения, которые могут потребоваться для решения судебного спора***	
7	***Решение по указанному делу***	

Задача 3

Гражданин Б. обратился в суд с иском к юридическому и физическому лицу о защите авторских прав, указав, что является автором каталога проектов ландшафтного дизайна (авторское право подтверждено свидетельством о депонировании), которые, в нарушение его авторских прав, размещены на сайте ответчика в сети «Интернет».

1. Раскройте сущность основных понятий.
2. Укажите, какие факты необходимо установить для принятия решения по данному делу (установите их).
3. Раскройте особенности содержания и применения принципа исчерпания права.
4. Раскройте особенности данного дела с указанием ссылок на соответствующие статьи.
5. Сформулируйте возможное решение по указанному делу.

Решение задачи (оформление ответов)

1	***Сущность основных понятий***	
2	***Факты, необходимые для принятия решения по данному делу:***	
3	***Принцип исчерпания права***	
4	***Возможность применения принципа исчерпания права к данному делу.***	
5	***Особенности дела:***	
6	***Решение по указанному делу***	

Задача 4

Автор служебного изобретения обратился в суд с иском к организации (работодателю) о выплате вознаграждения за использование разработанного им изобретения, компенсации за невыплату вознаграждения и возмещении расходов на оплату государственной пошлины.

Патент на изобретение был выдан организации 12 сентября 2003 г. На производстве организации изобретение было внедрено 10 февраля 2000 г (действие патента прекращено 4 апреля 2010 г.) и продолжают использоваться (отдельные признаки изобретения). Авторское вознаграждение за использование изобретения не выплачивается.

1. Раскройте сущность основных понятий.
2. Раскройте особенности данного дела с указанием ссылок на соответствующие статьи.

3. Укажите условия, необходимые для принятия решения по данному делу.

4. Сформулируйте возможное решение по указанному делу.

Решение задачи (оформление ответов)

1	***Сущность основных понятий***	
2	***Особенности дела***	
3	***Условия, необходимые для принятия решения по делу***	
4	***Решение по указанному делу***	

Задача 5

Юридическое лицо обратилось в арбитражный суд с иском к индивидуальному предпринимателю о защите исключительного права на товарный знак, а также о принятии обеспечительных мер в виде запрета ответчику совершать действия по передаче домена другому регистратору.

1. Раскройте сущность основных понятий.

2. Раскройте особенности данного дела с указанием ссылок на соответствующие статьи.

3. Укажите условия, необходимые для принятия решения по данному делу.

4. Сформулируйте возможное решение по указанному делу.

Решение задачи (оформление ответов)

1	***Сущность основных понятий***	
2	***Факты, необходимые для принятия решения по данному делу***	
3	***Особенности дела***	
4	***Решение по указанному делу***	

Практическая работа № 15

Тема. Административная и уголовная ответственность в сфере в сфере информационной безопасности

Цель занятия: Изучение основ правового регулирования общественных отношений в области конфиденциальной информации.

Теоретическая часть:

1. Понятие и виды информационных правоотношений

Одной из задач российского информационного законодательства является регулирование общественных отношений в определенных

действующими законами сферах. Информационные отношения, которые оказались урегулированными законом или сложились в результате такого регулирования, становятся информационными правоотношениями. Посредством информационных правоотношений поведение субъектов права канализируется в нужных государству направлениях. В силу этого категория информационных правоотношений имеет важнейшее значение для теории и практики информационного права.

Юридическая наука сравнительно недавно обратилась к анализу информационных правоотношений, используя для этих целей обычный набор концептуальных средств, предлагаемых теорией права, что предопределяет единство исходных установок и сказывается на общности методологических подходов к изучению данного феномена. Между тем указанная общность не способствовала выработке общепризнанного определения информационного правоотношения, его содержания и структуры. Сегодня существует множество самых различных точек зрения в этой, без преувеличения проблемной, области, которые имеют как содержательные пересечения, так и несовпадающие по принципиальным вопросам суждения.

Нормы информационного права регулируют далеко не все, а лишь наиболее важные, принципиальные группы общественных отношений, которые имеют существенное значение для интересов государства, общества и личности. Это прежде всего отношения, связанные с поиском, получением, передачей, производством, распространением, преобразованием и потреблением информации. Следует иметь в виду, что не любое отношение, сложившееся в информационной сфере, может быть подвергнуто правовому регулированию. Причинами тому являются, во-первых, нецелесообразность правового вмешательства в отдельные сферы жизнедеятельности и, во-вторых, невозможность внешнего контроля за исполнением тех либо иных нормативных предписаний в силу специфики объекта регулирования. Например, невозможно урегулировать нормами права процесс творчества, установить порядок создания произведения или запретить с положительным эффектом распространение анекдотов. Таким образом, не всякое общественное отношение, сложившееся в связи с поиском, получением, передачей, производством, распространением, преобразованием и потреблением информации, выступает в форме информационного правоотношения. В этой форме выступают лишь те реальные общественные отношения, которые урегулированы нормами информационного законодательства либо искусственно сформировались в результате такого регулирования. Информационное правоотношение в широком смысле есть, следовательно, реальное общественное отношение, урегулированное нормами информационного права.

В информационном праве, коль скоро это комплексная отрасль права, различаются регулятивные и охранительные информационные правоотношения. Правоотношения первого вида связаны с дозволенной деятельностью по поиску, получению, передаче, производству и распространению информации. Таковы, например, правоотношения,

складывающиеся в связи с доступом физических и юридических лиц к информации (ст. 8 Федерального закона "Об информации, информационных технологиях и о защите информации"). Данные правоотношения возникают из правомерных действий лиц, участвующих в процессе доступа. Правоотношения второго вида возникают в связи с совершенными правонарушениями. Так, за воспрепятствование распространению продукции средства массовой информации, виновные лица несут ответственность, согласно ст. 13.16 КоАП. Данные правоотношения возникают тогда, когда имеют место незаконные ограничения прав средств массовой информации.

Помимо деления информационных правоотношений на регулятивные и охранительные, их можно дифференцировать на материальные и процедурные правоотношения.

Материальные информационные правоотношения складываются по поводу реализации прав и обязанностей субъектов данных отношений. Примерами подобного рода правоотношений могут служить отношения, возникшие в результате реализации журналистом права быть принятым должностными лицами в связи с запросом информации (ст. 47 Закона РФ "О средствах массовой информации") либо в результате реализации права гражданина или организации на опровержение не соответствующих действительности и порочащих их честь и достоинство сведений (ст. 43 Закона РФ "О средствах массовой информации"). Процедурные информационные правоотношения складываются по поводу процедуры их возникновения, изменения или прекращения. Например, при оформлении граждан на допуск к особой важности, совершенно секретным и секретным сведениям (раздел 2 Инструкции о порядке допуска должностных лиц и граждан Российской Федерации к государственной тайне).

В зависимости от структуры связи между субъектами информационных правоотношений они делятся на абсолютные и относительные. В абсолютных информационных правоотношениях управомоченному субъекту противостоит неопределенное количество пассивно обязанных лиц, которые не вправе чинить никаких препятствий в реализации юридических возможностей управомоченного.

Примером абсолютного информационного правоотношения может служить правоотношение, складывающееся между обладателем секрета производства, наделенного исключительным правом на его использование и третьими лицами (п. 1 ст. 1466 ГК РФ, п.1 ст. 1229 ГК РФ).

Что касается абсолютных правоотношений собственности, возникающих по поводу информационных ресурсов, то их нельзя отнести к информационным в силу прямого указания законодателя, содержащегося в п. 5 ст. 11 Федерального закона "Об информации, информационных технологиях и о защите информации". В соответствии с указанным пунктом право собственности и иные вещные права на материальные носители, содержащие документированную информацию, устанавливаются гражданским законодательством.

В относительных информационных правоотношениях управомоченному субъекту в качестве обязанных противостоят точно поименованные лица. Таковы, например, отношения между работником и работодателем, складывающиеся по поводу персональных данных работника (гл. 14 Трудового кодекса РФ).

Состав информационных правоотношений, как собирательной категории, напрямую зависит от характера общественных отношений, составляющих предмет информационного права, а также от их отраслевой принадлежности. Поскольку основу предмета информационного права образуют отношения, связанные с поиском, получением, передачей, производством, распространением, преобразованием и потреблением информации, постольку, будучи урегулированными правовыми нормами, они и составят основную группу информационных правоотношений.

К этой группе примыкают правоотношения, складывающиеся по поводу управления информационными процессами, информатизацией и обеспечением информационной безопасности.

Структуру информационного правоотношения образуют его элементы, в качестве которых выделяются субъекты правоотношения, объекты правоотношения и содержание правоотношения, включающие субъективные права и юридические обязанности участников правоотношения.

2. Субъекты информационных правоотношений

Участниками информационных правоотношений выступают субъекты информационного права, под которыми понимаются физические и юридические лица, а также публичные образования, являющиеся носителями предусмотренных информационным законодательством прав и обязанностей. От имени РФ, субъекта РФ, муниципального образования правомочия обладателя информации осуществляются соответственно государственными органами и органами местного самоуправления в пределах их полномочий, установленных соответствующими нормативными правовыми актами. Из этого следует, что субъектами информационных правоотношений могут быть не всякие лица, а только те, которые наделены действующим законодательством определенными правами и обязанностями.

В правоотношениях, связанных с поиском и получением информации, которые складываются прежде всего по поводу использования документированной информации, организации и деятельности средств массовой информации, на первый план выходят фигуры потребителей информации, т.е. тех лиц, которые реализуют свое конституционное право на поиск и получение информации. В этот круг входят граждане, организации, органы государственной власти и местного самоуправления, в том числе пользователи библиотек, журналисты, потребители рекламы. Участниками данных правоотношений являются, кроме того, обладатели информации.

В правоотношениях, связанных с производством информации, которые складываются по поводу деятельности средств массовой информации, рекламной деятельности, ведущую роль играют производители информации.

Это прежде всего издательства, редакции средств массовой информации, рекламодатели, рекламопроизводители, журналисты, авторы произведений и объектов технического творчества, органы государственной власти и местного самоуправления.

В правоотношениях, связанных с передачей и распространением информации, которые складываются преимущественно в области связи, сферах рекламной деятельности и международного информационного обмена, их участниками выступают организации связи, операторы связи, пользователи услуг связи, рекламораспространители, лица, участвующие в международном информационном обмене.

В правоотношениях, связанных с управлением информационными процессами, которые складываются практически во всей информационной сфере, главенствующую роль играют органы государственного управления в информационной сфере. Это в первую очередь Правительство РФ, Министерство информационных технологий и связи РФ, Министерство культуры и массовых коммуникаций РФ, Федеральная служба по интеллектуальной собственности, патентам и товарным знакам, Федеральное архивное агентство, Федеральное агентство по информационным технологиям, Федеральное агентство связи и, кроме того, ряд координационных органов, обеспечивающих согласованность действий органов государственной власти. В числе последних следует выделить Межведомственную комиссию по защите государственной тайны.

В правоотношениях, связанных с обеспечением информационной безопасности, которые складываются по поводу жизненно важных интересов личности, общества и государства, видное место занимают Правительство РФ, Совет Безопасности РФ, Федеральная служба безопасности РФ, Служба специальной связи и информации при Федеральной службе охраны РФ, Федеральная служба по техническому и экспортному контролю РФ, Государственная фельдъегерская служба РФ, Межведомственная комиссия по защите государственной тайны.

В правоотношениях, связанных с созданием и использованием информационных технологий, систем и сетей, а также с процессами информатизации, которые складываются по поводу разработки и применения информационных технологий и средств их обеспечения, принимают участие Министерство информационных технологий и связи РФ, Федеральная служба по надзору в сфере связи, Федеральное агентство по информационным технологиям, Федеральное агентство связи, органы по сертификации и испытательные центры, организации, занимающиеся выполнением научно-исследовательских, опытно-конструкторских и технологических работ в области информационных технологий.

К участникам информационных правоотношений могут быть отнесены и иные, помимо названных выше, субъекты. Их круг по мере развития и совершенствования информационного законодательства постоянно расширяется. Кроме того, один субъект может выступать участником

информационных правоотношений, складывающихся в различных областях общественной жизни и деятельности.

3. Объекты информационных правоотношений

Вопрос об объекте правоотношения является одним из ключевых и в то же время одним из наиболее спорных в юридической науке. На сегодняшний день сложились три группы основных точек зрения на объект правоотношения.

В основу первой из них положена монистическая концепция объекта, полагающая в качестве такового действия или поведение субъекта, направленное на определенные материальные блага, поскольку только действие субъекта может быть подвергнуто правовому воздействию.

В основе второй группы точек зрения лежит плюралистическая концепция объекта, предполагающая множественность объектов, их разнообразие, которое отражает всю палитру регулируемых общественных отношений. В рамках данной концепции в качестве объекта правоотношений рассматриваются материальные и нематериальные блага, продукты духовного творчества и т.п.

Представители третьей концепции обосновывают свои взгляды на объект правоотношения, исходя из понимания его как правового режима.

Под объектами информационных правоотношений мы понимаем блага, существующие в формах информации, документированной информации и информационных систем, по поводу которых возникает и осуществляется деятельность участников этих правоотношений. При этом информация является благом особого рода, а документированная информация и информационные системы - благами материальными.

Не останавливаясь на особенностях информации и ее документированной разновидности, которые показаны нами в других главах настоящего учебника, дадим краткую характеристику информационных систем.

Под информационной системой законодатель понимает организационно упорядоченную совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств.

Понятие информационной системы весьма сложное и противоречивое как с технической, так и с юридической точки зрения. Законодатель, вводя термин "информационная система", избрал традиционный путь, следуя представлениям о системе как совокупности взаимосвязанных элементов. Между тем юридическая конструкция информационной системы напоминает юридическую конструкцию предприятия как самостоятельного объекта прав, признаваемого недвижимостью. Аналогия в данном случае состоит в том, что не только сама информационная система выступает в качестве самостоятельного объекта информационного правоотношения, но и образующие ее элементы. Действовавшее ранее информационное законодательство не содержало исчерпывающего перечня информационных систем и тем более их структурных элементов. Федеральным законом "Об

информации, информатизации и защите информации" к разновидностям информационных систем были отнесены:

- библиотеки;
- архивы;
- фонды;
- банки данных;
- другие информационные системы.

Такое решение законодателя нельзя признать удачным, поскольку библиотеки и архивы, являясь по определению учреждениями, не подпадают под родовое понятие информационной системы. Действительно, в соответствии со ст. 1 Федерального закона "О библиотечном деле" библиотека представляет собой информационное, культурное, образовательное учреждение, располагающее организационным фондом тиражированных документов и предоставляющее их во временное пользование физическим и юридическим лицам. А архив (п. 9 ст. 3 Федерального закона "Об архивном деле в Российской Федерации") - это учреждение или структурное подразделение организации, осуществляющее хранение, комплектование, учет и использование архивных документов.

Исходя из признания многообразия информационных систем в литературе, предлагается их классификация. Различают следующие виды информационных систем:

- открытые (для общего пользования) и закрытые (для ограниченного круга);
- государственные и негосударственные (корпоративные);
- национальные и международные;
- малые, средние и крупные информационные системы.

Действующее информационное законодательство дифференцирует информационные системы по их принадлежности субъекту, принявшему решение об их создании.

Согласно ст. 13 Федерального закона "Об информации, информационных технологиях и о защите информации" информационные системы включают в себя:

- государственные информационные системы;
- муниципальные информационные системы;
- иные информационные системы.

В свою очередь государственные информационные системы подразделяются на федеральные и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов РФ или правовых актов государственных органов.

Муниципальные информационные системы представляют собой системы, созданные на основании решения органа местного самоуправления.

Иные информационные системы - это системы, создаваемые операторами систем, не являющихся государственными или муниципальными системами.

Государственные информационные системы создаются в целях реализации полномочий государственных органов и обеспечения обмена информацией между этими органами, а также в иных установленных федеральным законом целях. При создании государственных информационных систем должны соблюдаться требования, предусмотренные Федеральным законом "О размещении заказов на поставки товаров, выполнение работ, оказание услуг для государственных и муниципальных нужд".

Государственные информационные системы создаются и эксплуатируются на основе статистической и иной документированной информации, предоставляемой гражданами, организациями, государственными органами, органами местного самоуправления.

Перечни видов информации, предоставляемой в обязательном порядке, устанавливаются федеральными законами, а условия ее предоставления - Правительством РФ или соответствующими государственными органами, если иное не предусмотрено федеральными законами.

Правительство РФ вправе устанавливать обязательные требования к порядку ввода в эксплуатацию отдельных государственных информационных систем.

Не допускается эксплуатация государственной информационной системы без надлежащего оформления прав на использование ее компонентов, являющихся объектами интеллектуальной собственности.

Технические средства, предназначенные для обработки информации, содержащейся в государственных информационных системах, в том числе программно-технические средства и средства защиты информации, должны соответствовать требованиям законодательства РФ о техническом регулировании.

4. Содержание информационных правоотношений

Важнейший характеристикой любого правоотношения является взаимодействие его участников, которое проявляется в реализации их взаимных прав и обязанностей. Права и обязанности участников информационных правоотношений составляют юридическое содержание последних.

Под правами участников (субъектов) информационных правоотношений понимается мера возможного или дозволенного поведения данного лица. Например, любое лицо может использовать общедоступную информацию по своему усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации (п. 2 ст. 7 Федерального закона "Об информации, информационных технологиях и о защите информации").

Права субъектов информационных правоотношений (субъективные информационные права) имеют общую внутреннюю структуру, которая проявляется в наличии следующих трех основных элементов:

− правомочие на собственные действия, заключающееся в возможности совершения фактических и юридически значимых действий;

− правомочие на чужие действия, заключающееся в возможности требовать от обязанного лица исполнения возложенных на него обязанностей;

− правомочие на защиту, заключающееся в возможности прибегнуть к государственно-принудительным мерам в случае нарушения субъективного права либо неисполнения одним из участников правоотношения своих обязанностей.

Примером правомочия на собственные действия может служить правило п. 3 ст. 6 Федерального закона "Об информации, информационных технологиях и о защите информации", в соответствии с которым обладатель информации, если иное не предусмотрено федеральными законами, вправе, в частности:

− разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа;

− использовать информацию, в том числе распространять ее, по своему усмотрению;

− передавать информацию другим лицам по договору или на ином установленном законом основании.

Субъективное информационное право выступает как право требования, например, в случае притязания абонента, касающегося переключения абонентского номера на абонентскую линию в помещении, расположенном по другому адресу и находящемуся во владении данного абонента (п. 4 ст. 45 Федерального закона "О связи").

Возможность прибегнуть к государственному принуждению в случае нарушения субъективного права предусмотрена, например, правилом ст. 62 Закона РФ "О средствах массовой информации", в соответствии с которым моральный (неимущественный) вред, причиненный гражданину в результате распространения средством массовой информации не соответствующих действительности сведений, порочащих честь и достоинство гражданина либо причинивших ему иной неимущественный вред, возмещается по решению суда средством массовой информации, а также виновными должностными лицами и гражданами в размере, определяемом судом.

Под обязанностью участника информационного правоотношения понимается установленная законом мера должного или требуемого поведения, которой, как правило, корреспондирует субъективное право другого лица. Как и субъективное информационное право, юридическая обязанность обладает внутренней структурой, которая характеризуется наличием следующих элементов:

− необходимостью совершить определенные действия либо воздержаться от них;

− необходимостью исполнить требования управомоченного субъекта;

− необходимостью нести ответственность за нарушение субъективных прав других участников правоотношения или за неисполнение их законных требований.

Примером необходимости совершить определенные действия будет являться требование, установленное ст. 7 Федерального закона "Об

обязательном экземпляре документов", согласно которому производители документов доставляют через полиграфические организации в федеральный орган исполнительной власти по вопросам печати, телерадиовещания и средств массовых коммуникаций по одному обязательному федеральному экземпляру всех видов печатных изданий в день выхода в свет первой партии тиража.

Необходимость исполнения требований управомоченного лица может быть продемонстрирована правилом ст. 21 Закона РФ "О государственной тайне", в соответствии с которым допуск должностных лиц и граждан к государственной тайне требует от них, в частности, принятия на себя обязательств перед государством по нераспространению доверенных им сведений, составляющих государственную тайну, и письменного согласия на проведение в отношении их уполномоченными органами проверочных мероприятий.

Ответственность за нарушение субъективных прав другого участника информационного правоотношения предусмотрена, в частности, ст. 19.7 КоАП, согласно которой непредоставление или несвоевременное предоставление в государственный орган (должностному лицу) сведений (информации), предоставление которых предусмотрено законом и необходимо для осуществления этим органом (должностным лицом) его законной деятельности, влечет наложение административного штрафа на граждан в размере от одного до трех минимальных размеров оплаты труда; на должностных лиц - от трех до пяти минимальных размеров оплаты труда; на юридических лиц - от тридцати до пятидесяти минимальных размеров оплаты труда.

Возможное и должное поведение участников информационного правоотношения выражает состояние их связанности. При этом каждый из субъектов правоотношения чаще всего одновременно обладает правом и несет обязанности, например, в правоотношении, складывающемся между библиотекой и пользователем библиотеки (ст. 7, 9, 12, 13 Федерального закона "О библиотечном деле").

Не подвергая анализу все разнообразие субъективных информационных прав и субъективных информационных обязанностей, очертим круг наиболее значимых из них.

Важнейшими в содержании информационного правоотношения являются конституционные права на поиск, получение, передачу, производство и распространение информации. Эти права реализуются, прежде всего, через средства массовой информации и глобальную сеть Интернет, которые в настоящее время являются наиболее доступным способом поиска, получения и распространения общественно значимых сведений.

С конституционными информационными правами тесно связаны права на создание произведений науки, литературы, искусства и произведений технического творчества, право на создание средств массовой информации, информационных систем, сетей и средств их обеспечения, право на защиту личности от воздействия недостоверной и ложной информации.

Среди обязанностей в информационном правоотношении выделим обязанности органов государственной власти и местного самоуправления по предоставлению документированной информации ее потребителям, по достоверному, оперативному и полному информированию населения, по обеспечению гарантий свободы слова, обязанности по подготовке и представлению обязательных экземпляров документов.

Методические рекомендации по выполнению практического занятия

ПОРЯДОК ВЫПОЛНЕНИЯ

1. Выбрать задание согласно представленному в таблице делению на подгруппы (задание указано в таблице).

1 подгруппа *ФЗ РФ № 149*		**4 подгруппа *ФЗ РФ № 126 (выбираем субъектов из статей: 3-24)***
1		
2		
3		
4		
5		
2 подгруппа *ФЗ РФ № 152*		5 подгруппа *ФЗ РФ № 5485-1*
1		
2		
3		
4		
5		
3 подгруппа *ФЗ РФ № 98*		**6 подгруппа *ФЗ РФ № 126 (выбираем субъектов из статей: 25-49)***
1		
2		
3		
4		
5		
7 подгруппа *ФЗ РФ № 126 (выбираем субъектов из статей: 50-74)*		**8 подгруппа *ФЗ РФ № 5485-1***
1		
2		
3		
4		
5		

2. Выполнить представленные задания.

3. Ответы на задание 3.2 представить в виде таблицы.

4. Цитаты, приведенные из НПА, подтверждать ссылками (абз. , п. , ч. , ст. , НПА).

Содержание отчета о практическом занятии

1. Цель работы.

2. Результат выполнения работы.

3. Выводы.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ВЫПОЛНЕНИЕ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ

1. Составить перечень субъектов правовых отношений в подгруппе (задание для подгрупп), привести закрепленное законодательно определение.

2. Указать правосубъектность одного из субъектов правовых отношений (субъекты, выбранные участниками одной из подгрупп, не должны повторяться).

3. Провести анализ правового статуса одного из субъектов.

3.1. Необходимо указать отдельно права субъекта.

3.2.Необходимо указать обязанность субъекта и соответственно ответственность, которая может быть применена в случае невыполнения каждой из приведенных обязанностей.

Обязанность субъекта	Ответственность

Практическая работа № 16

Тема. Перечень видов деятельности предприятий в области защиты информации, подлежащих лицензированию

Цель занятия: Получение навыков работы с национальными российскими и международными стандартами в области обеспечения информационной безопасности.

Теоретическая часть:

В состав законодательства по обеспечению информационной безопасности включаются федеральные законы, подзаконные нормативные правовые акты федеральных органов исполнительной власти, законы и подзаконные нормативные правовые акты субъектов Российской Федерации. К числу наиболее значимых нормативных правовые актов в области обеспечения информационной безопасности относятся следующие законы и подзаконные акты. Конституция Российской Федерации содержит нормы, которые определяют правовые основы информационной безопасности: основные положения правового статуса субъектов информационных отношений, принципы информационной безопасности (законности, уважения прав, баланс интересов личности, общества и государства), конституционный статус государственных органов, обеспечивающих информационную безопасность и др. Например, к таким положениям относятся нормы, которые устанавливают право каждого субъекта свободно искать, получать, передавать, производить и распространять информацию любым законным способом (п.4.ст. 29). Это конституционное право, устанавливающее возможность удовлетворения интересов личности и общества сбалансировано необходимостью их ограничения федеральным законом в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства (п.3.ст.55). Конституция Российской Федерации устанавливает запрет на доступ к информации о частной жизни и передачу сообщений по линиям телефонной связи (ст.23). Федеральный закон от 28 декабря 2010 г. N

390-ФЗ «О безопасности» закрепляет правовые основы обеспечения безопасности личности, общества и государства, определяет систему безопасности и ее функции, устанавливает порядок организации и финансирования органов обеспечения безопасности, а также контроля и надзора за законностью их деятельности. Закон определяет ключевые термины в области безопасности, которые применимы и для сферы информационной безопасности, принципы и систему безопасности, правовой статус и состав Совета Безопасности Российской Федерации. Федеральный закон от 27.07.2006, г., № 149-ФЗ «Об информации, информационных технологиях и о защите информации» фиксирует базовые нормы для всей системы информационного законодательства, в т.ч. правового обеспечения информационной безопасности. Они определяют основные термины и их определения, принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации (ст.3), классификацию информации по категориям доступа - общедоступную и ограниченного доступа (ст. 5), порядку ее предоставления или распространения (свободно распространяемую, обязательного предоставления или распространения, ограниченного распространения или запрещаемую для распространения вообще). Закон определяет базовые положения правового режима доступа к информации (ст.8) и его ограничения (ст.9), основные параметры правовых режимов распространения (ст.10) и документирования (ст.11) информации, информационных систем (ст.13), информационно- телекоммуникационных сетей (ст.15) и общие условия защиты информации (ст.16), информационных систем (ст.13) и использования информационных технологий, а также в общих чертах описывает ответственность за правонарушения в сфере информации, информационных технологий и защиты информации. Федеральный закон от 21 июня 1993 № 5485-1 «О государственной тайне», Федеральные законы от 29 июля 2004 № 98-ФЗ «О коммерческой тайне» и от 27.07.2006 г. № 152-ФЗ «О персональных данных» устанавливают правовые режимы информации ограниченного доступа, в том числе, сведений, составляющих государственную и коммерческую тайну. Нормы названных законов на более конкретном уровне, чем норма ст.9 закона «Об информации» регулируют формирование условий правового режима доступа к сведениям конфиденциального характера, конкретизируют правовой статус субъектов отношений, возникающих по поводу тайн и персональных данных. Именно в названных законах содержатся основные запреты, ограничения и дозволения, которые составляют правовые основания для формулировок составов информационных правонарушений, направленных на интересы личности, общества и государства в области конфиденциальности информации. Федеральный закон от 6 апреля 2011 г. № 63-ФЗ «Об электронной подписи». Нормы названного закона определяют правовой режим технологического обеспечения защиты информации в системе базовых законов информационного законодательства. В ст. 1 этого закона определена его цель - обеспечение правовых условий использования электронной цифровой подписи в электронных документах, при соблюдении

которых электронная цифровая подпись в электронном документе признается равнозначной собственноручной подписи в документе на бумажном носителе. В законе сформулированы функции электронной цифровой подписи: удостоверяющая, защитная и устанавливающая. Уголовный кодекс РФ в главе 28 Кодекса предусматривает ответственность за совершение преступлений в сфере компьютерной информации (ст.272-275). Всего в тексте Кодекса содержится более 50 отдельных статей, устанавливающих уголовную ответственность за нарушение установленных запретов в информационной сфере. Трудовой кодекс РФ устанавливаетправовой режим персональных данных работника, определяет общие требования по их обработке и защите, устанавливает сроки хранения таких данных и процедуру их использования. В случаях нарушения норм, регулирующих получение, обработку и защиту персональных данных работника, виновные лица привлекаются к дисциплинарной, материальной, административной, гражданско-правовой и уголовной ответственности. Трудовой кодекс РФ определяет норму об ответственности за разглашение отдельных видов тайн и персональных данных. КоАП РФ в главе 13 определяет административную ответственность за правонарушения в области связи и информации посвящена отдельная глава (ст. 13.1-13.24). В него включены еще более 90 статей, в которых определяется ответственность за совершение проступков информационного характера. Так, например, устанавливается ответственность за отказ в предоставлении гражданину информации (ст. 5.39), за сокрытие или искажение экологической информации (ст. 8.5), за незаконные действия по получению и (или) распространению информации, составляющей кредитную историю (ст. 5.53). Имеется также массив нормативных правовых актов подзаконного характера, состоящий из большого количества документов, регулирующих отдельные направления правового обеспечения информационной безопасности. Указ Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена». В данном Указе устанавливается запрет подключения информационных систем, информационно-телекоммуникационных сетей и средств вычислительной техники, применяемых для хранения, обработки или передачи информации, содержащей сведения, составляющие государственную тайну к информационнотелекоммуникационным сетям международного информационного обмена. В целях защиты информации государственные органы обязаны использовать только средства защиты информации, прошедшие сертификацию в Федеральной службе безопасности Российской Федерации и (или) получившие подтверждение соответствия в Федеральной службе по техническому и экспортному контролю. Выполнение данных требований Указа в полной мере должно обеспечить защиту информации, составляющей государственную тайну. Приказом ФСО России от 07.08.2009 N 487утвержденоПоложение о сегменте информационно-телекоммуникационной сети Интернет для федеральных органов

государственной власти и органов государственной власти субъектов Российской Федерации. Эксплуатацию, поддержание и развитие сегмента информационнотелекоммуникационной сети Интернет для федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации обеспечивает Служба специальной связи и информации ФСО России. В соответствии с названным нормативным правовым актом Сегмент сети Интернет – это находящаяся в ведении (эксплуатации) Федеральной службы охраны Российской Федерации (далее именуется - оператор сегмента сети Интернет) часть информационнотелекоммуникационной сети, связывающей информационные системы, информационнотелекоммуникационные сети различных государств посредством сетевых адресов информационно-телекоммуникационной сети Интернет (далее именуется - сеть Интернет). Сегмент сети Интернет предназначен для обеспечения размещения информации о деятельности Администрации Президента Российской Федерации, Аппарата Совета Федерации Федерального Собрания Российской Федерации, Аппарата Государственной Думы Федерального Собрания Российской Федерации, Аппарата Правительства Российской Федерации, аппаратов Конституционного Суда Российской Федерации, Верховного Суда Российской Федерации, Высшего Арбитражного Суда Российской Федерации, Генеральной прокуратуры Российской Федерации и Следственного комитета при прокуратуре Российской Федерации, федеральных органов государственной власти и органов государственной власти субъектов Российской Федерации, а также для доступа к сети Интернет должностных лиц указанных государственных органов (далее именуются - пользователи сегмента сети Интернет). Функционирование сегмента сети Интернет обеспечивается путем применения стандартных протоколов сети Интернет и регламентов обмена информацией в порядке, определяемом оператором сегмента сети Интернет. В российском правовом пространстве длительное время в обороте используется «служебная информация ограниченного распространения» о деятельности органов государственной власти, которая нередко упоминается в нормативных правовых актах как «служебная тайна». Постановление Правительства РФ № 1233 от 3 ноября 1994 г. «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах государственной власти» (95) определяется правовое положение информации ограниченного доступа, несмотря на то, что п.п.1 и 4 ст.9 ФЗ «Об информации» ограничение доступа к информации и, в частности, отнесение информации к сведениям, составляющим служебную тайну, устанавливаются исключительно федеральными законами. Явное несовершенство информационного законодательства и практики его применения отрицательно влияет на состояние правовой защиты интересов субъектов правоотношений. Пробел в нормативных правовых актах, устанавливающих оборот информации служебного характера, не позволяет установить запрет либо ограничения на ее использование, а вместе с этим создает ситуацию невозможности установить

административную и / или уголовную ответственность за нарушения порядка распространения этой важной формы информации.

Методические рекомендации по выполнению практического занятия

ПОРЯДОК ВЫПОЛНЕНИЯ

1. Выполнение поиска информации согласно индивидуальному заданию.
2. Ответ на контрольный вопрос согласно последней цифре варианта по журналу.
3. Выполнение, оформление и защита отчета о практическом занятии

Содержание отчета о практическом занятии

В отчете следует указать:

1. Цель работы;
2. Результат выполнение индивидуального задания;
3. Ответы на контрольные вопросы;
4. Выводы по проделанной работе.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ВЫПОЛНЕНИЕ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ

1. Описать сущность и значение, назвать виды административного и технического регулирования, в том числе в области ИБ.

Выбрать предметную область

1	Лицензирование
2	Лицензирование технической защиты конфиденциальной информации
3	Лицензирование деятельности по разработке и производству средств защиты конфиденциальной информации
4	Сертификация
5	Декларирование соответствия
6	Техническое регламентирование
7	Идентификационная экспертиза
8	Контроль
9	Контроль за проведением независимой идентификационной экспертизы товаров и технологий

2. Описать сущность данного регулирования в области ИБ.
3. Указать цель в рамках данного регулирования в области ИБ.
4. Указать соответствующие НПА ().

НПА	**Краткое содержание соответствующего положения НПА**

5. Охарактеризовать правосубъектность участников правовых отношений в рамках данного регулирования в области ИБ.

Управомоченный субъект	Правосубъектность управомоченного лица	Права субъекта	Обязанный субъект	Действия, осуществляемые в отношении управомоченного лица
I	II	III	IV	V

Содержание колонок I и IV должно соответствовать

6. Описать порядок действий при реализации данного регулирования в области ИБ.

Практическая работа № 17

Тема. Порядок сертификации средств защиты информации

Цель занятия: Получение навыков работы с национальными российскими и международными стандартами в области обеспечения информационной безопасности.

Теоретическая часть:

Система стандартов по защите информации (ССЗИ) - совокупность взаимосвязанных стандартов, устанавливающих характеристики продукции, правила осуществления и характеристики процессов, выполнения работ или оказания услуг в области защиты информации.

Национальные стандарты (ГОСТы) в общем случае являются рекомендательными. Однако в ряде случаев обязательность следования стандартам и спецификациям закреплена законодательно. В соответствии со ст.6 ФЗ №162 "О стандартизации в Российской Федерации" в том случае, если речь идет о "стандартизации в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, продукции, для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, а также в отношении процессов и иных объектов стандартизации, связанных с такой продукцией", стандарты являются обязательными к применению.

Основополагающим стандартом РФ в области защиты информации (некриптографическими методами) является ГОСТ Р 52069.0-2013 "Защита информации. Система стандартов. Основные положения".

Целью создания ССЗИ является достижение рациональной упорядоченности организации и содержания работ в области ЗИ, повышение эффективности ЗИ на основе установления общих правил и характеристик для их многократного использования, а также повышение эффективности работ по стандартизации за счет упорядочения структуры системы стандартов,

процесса разработки стандартов, учета взаимосвязи стандартов различных систем.

Основными задачами по формированию и развитию ССЗИ являются:

− установление основополагающих принципов построения, требований к составу и содержанию системы документов в области ЗИ;

− обеспечение единства терминологии в области ЗИ;

− упорядочение объектов и аспектов стандартизации в области ЗИ;

− обеспечение единства организационных и методических подходов к проведению работ по ЗИ;

− установление системы требований по ЗИ, предъявляемых к различным видам ОЗИ, и методов контроля выполнения этих требований;

− установление общих технических требований к СЗИ и СКЭЗИ, методам их испытаний;

− установление общих требований к услугам по ЗИ;

− установление требований к методам и методикам испытаний и оценки качества СЗИ и СКЭЗИ, к методам и методикам измерений в процессе контроля эффективности мероприятий по ЗИ;

− установление требований к метрологическому, информационному и другим видам обеспечения ЗИ.

Система стандартов по защите информации включает следующие виды документов в области стандартизации по ЗИ, используемых на территории Российской Федерации:

− национальные стандарты Российской Федерации, в том числе ограниченного распространения, государственные военные стандарты, национальные стандарты, оформленные на основе аутентичных переводов международных стандартов (гармонизированные стандарты);

− межгосударственные стандарты;

− правила стандартизации, нормы и рекомендации в области стандартизации;

− общероссийские классификаторы технико-экономической и социальной информации;

− стандарты организаций;

− предварительные национальные стандарты

Методические рекомендации по выполнению практического занятия

ПОРЯДОК ВЫПОЛНЕНИЯ

1. Выполнение поиска информации согласно индивидуальному заданию.

2. Ответ на контрольный вопрос согласно последней цифре варианта по журналу.

3. Выполнение, оформление и защита отчета о практическом занятии

Содержание отчета о практическом занятии

В отчете следует указать:

1. Цель работы;

2. Результат выполнение индивидуального задания;

3. Ответы на контрольные вопросы;
4. Выводы по проделанной работе.

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ВЫПОЛНЕНИЕ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ

Выполнить поиск разделов в нормативных источниках в соответствии со своим вариантом по журналу (таблица 1). Результаты поиска свести в таблицу и вставить в отчет.

Таблица 1 – Темы индивидуального задания

№	Тема
1	Управление доступом к внутренней сети
2	Политика информационной безопасности
3	Обеспечение непрерывности основного процесса организации
4	Антивирусная защита
5	Аудит информационной безопасности
6	Защита носителей информации
7	Реализация механизмов идентификации и аутентификации
8	Управление инцидентами информационной безопасности
9	Использование криптографических средств защиты
10	Контроль и управление доступом
11	Обеспечение целостности защищаемой информации
12	Сетевое администрирование
13	Защита персональных данных сотрудников
14	Безопасная передача данных
15	Защита коммерческой информации
16	Управление активами организации
17	Защита приложений
18	Использование биометрических средств защиты информации

РЕКОМЕНДАЦИИ

Обратите внимание на статус нормативного документа (возможна его замена, отмена, выпуск новой версии).

СПИСОК РЕКОМЕНДУЕМЫХ НОРМАТИВНЫХ ДОКУМЕНТОВ

1. ГОСТ Р ИСО/МЭК 27000-2012: Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.
2. ГОСТ Р ИСО/МЭК 27001-2005: Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
3. ГОСТ Р ИСО/МЭК 27002-2005: Информационные технологии. Свод правил по управлению защитой информации.
4. ГОСТ Р ИСО/МЭК 27003-2012: Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.
5. ГОСТ Р ИСО/МЭК 27004-2009: Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения.
6. ГОСТ Р ИСО/МЭК 27005-2008: Информационная технология. Методы обеспечения безопасности. Менеджмент рисков безопасности информации.
7. ГОСТ Р ИСО/МЭК 27006-2008: Информационные технологии. Методы и средства обеспечения безопасности. Требования для органов, обеспечивающих аудит и сертификацию систем менеджмента информационной безопасности.
8. ГОСТ Р ИСО/МЭК 27007-2011: Информационные технологии. Методы и средства обеспечения безопасности. Руководящие указания по аудиту систем менеджмента систем информационной безопасности.
9. ГОСТ Р 56045 – 2014/ISO/IEC TR 27008-2011: Информационная технология. Методы и средства обеспечения безопасности. Рекомендации для аудиторов в отношении мер и средств контроля и управления информационной безопасностью.
10. ГОСТ Р ИСО/МЭК 27011-2012: Информационные технологии. Методы защиты. Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги, на основе ISO/IEC 27002.
11. ГОСТ Р ИСО/МЭК 27031-2012: Информационная технология. Методы и средства обеспечения безопасности. Руководство по готовности информационно-коммуникационных технологий к обеспечению непрерывности бизнеса.

12. ГОСТ Р ИСО/МЭК 27033 -1-2009: Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 1 Обзор и концепции.
13. ГОСТ Р ИСО/МЭК 27033 -2-2012: Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 2 Руководство по разработке и реализации сетевой безопасности.
14. ГОСТ Р ИСО/МЭК 27033 -3-2010: Информационная технология. Методы и средства обеспечения безопасности. Сетевая безопасность. Часть 3 Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления.
15. ГОСТ Р ИСО/МЭК 27034 -1-2014: Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия.
16. ГОСТ Р ИСО/МЭК 27035-2011: Информационные технологии. Метод обеспечения безопасности. Управление случайностями в системе информационной безопасности.
17. ГОСТ Р ИСО/МЭК 17799-2005: Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по менеджменту информационной безопасности.
18. ГОСТ Р ИСО/МЭК 13569-2005: Услуги финансовые. Руководящие указания по обеспечению информационной безопасности.
ГОСТ Р ИСО/МЭК 15408- 3-2008: Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ. Часть 3. Требования к обеспечению защиты.
19. ГОСТ Р ИСО/МЭК 18045-2008: Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности ИТ
20. ГОСТ Р ИСО/МЭК 18028-3-2005: Информационные технологии. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 3. Коммуникации для обеспечения безопасности между сетями с применением шлюзов безопасности.
21. ГОСТ Р ИСО/МЭК 18028-4-2005: Информационные технологии. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 4. Обеспечение безопасности удаленного доступа.
22. ГОСТ Р ИСО/МЭК 18028-4-2006: Информационные технологии. Методы и средства обеспечения безопасности. Безопасность информационной сети. Часть 5. Коммуникации для обеспечения безопасности между сетями с применением виртуальных частных систем.
23. ГОСТ Р ИСО/МЭК 13335-1-2004: Информационная технология. Методы обеспечения безопасности. Управление безопасностью информационных и телекоммуникационных технологий. Часть 1. Концепция и модели управления безопасностью информационных и телекоммуникационных технологий.

24. ГОСТ Р ИСО/МЭК ТО 13335-5-2006: Информационная технология. Методы и средства обеспечения безопасности. Часть 5. Руководство по менеджменту безопасности сети.

25. BS 7799- 3-2006: Практические правила управления информационной безопасностью.

26. BS 7799- 2-2002: Спецификация системы управления информационной безопасностью.

27. Рекомендация МСЭ-Т X.805 «Архитектура безопасности для систем, обеспечивающих связь между оконечными устройствами».

28. Рекомендация МСЭ-Т серии X.8xx.

29. ГОСТ Р 52448-2005: Защита информации. Обеспечение безопасности сетей электросвязи. Общие положения.

30. СТО БР ИББС-1.1-2007 Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Аудит информационной безопасности».

31. СТО БР ИББС-1.0-2010 Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».

32. СТО БР ИББС-1.2-2010 Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки соответствия информационной безопасностиорганизаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0 – 2010».

33. РС БР ИББС-2.0-2007 Рекомендации в области стандартизации Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0».

34. РС БР ИББС-2.1-2007 Рекомендации в области стандартизации Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Руководство по самооценке соответствия информационной безопасности организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0».

35. РС БР ИББС-2.2-2009 Рекомендации в области стандартизации Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методика оценки рисков нарушения информационной безопасности».

36. РС БР ИББС-2.3-2010 Рекомендации в области стандартизации Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Требования по обеспечению безопасности персональных данных в информационных системах персональных данных организаций банковской системы Российской Федерации».

37. РС БР ИББС-2.4-2010 Рекомендации в области стандартизации Банка России: «Обеспечение информационной безопасности организаций

банковской системы Российской Федерации. Отраслевая частная модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных организаций банковской системы Российской Федерации».

38. Стандарт безопасности данных индустрии платежных карт PCI DSS версия (3.0 -).

39. «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (утв. Банком России 09.06.2012 N 382-П) (ред. от 14.08.2014).

40. ISO 27799:2008 - Информатика в здравоохранении. Менеджмент безопасности информации по стандарту ISO/IEC 27002.

41. ISO/IEC 24762:2008 - Информационные технологии - Методы обеспечения защиты – Рекомендации по услугам восстановления после чрезвычайных ситуаций функций и механизмов безопасности информационных и телекоммуникационных технологий.

Практическая работа № 18

Тема. Анализ стандартов информационной безопасности

Цель занятия: Ознакомиться со стандартом, получить навыки его использования при организации информационной безопасности.

Теоретическая часть:

Система стандартов по защите информации (ССЗИ) - совокупность взаимосвязанных стандартов, устанавливающих характеристики продукции, правила осуществления и характеристики процессов, выполнения работ или оказания услуг в области защиты информации.

Национальные стандарты (ГОСТы) в общем случае являются рекомендательными. Однако в ряде случаев обязательность следования стандартам и спецификациям закреплена законодательно. В соответствии со ст.6 ФЗ №162 "О стандартизации в Российской Федерации" в том случае, если речь идет о "стандартизации в отношении оборонной продукции (товаров, работ, услуг) по государственному оборонному заказу, продукции, используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с законодательством Российской Федерации иной информации ограниченного доступа, продукции, сведения о которой составляют государственную тайну, продукции, для которой устанавливаются требования, связанные с обеспечением безопасности в области использования атомной энергии, а также в отношении процессов и иных объектов стандартизации, связанных с такой продукцией", стандарты являются обязательными к применению.

Основополагающим стандартом РФ в области защиты информации (некриптографическими методами) является ГОСТ Р 52069.0-2013 "Защита информации. Система стандартов. Основные положения".

Целью создания ССЗИ является достижение рациональной упорядоченности организации и содержания работ в области ЗИ, повышение эффективности ЗИ на основе установления общих правил и характеристик для их многократного использования, а также повышение эффективности работ по стандартизации за счет упорядочения структуры системы стандартов, процесса разработки стандартов, учета взаимосвязи стандартов различных систем.

Основными задачами по формированию и развитию ССЗИ являются:

− установление основополагающих принципов построения, требований к составу и содержанию системы документов в области ЗИ;

− обеспечение единства терминологии в области ЗИ;

− упорядочение объектов и аспектов стандартизации в области ЗИ;

− обеспечение единства организационных и методических подходов к проведению работ по ЗИ;

− установление системы требований по ЗИ, предъявляемых к различным видам ОЗИ, и методов контроля выполнения этих требований;

− установление общих технических требований к СЗИ и СКЭЗИ, методам их испытаний;

− установление общих требований к услугам по ЗИ;

− установление требований к методам и методикам испытаний и оценки качества СЗИ и СКЭЗИ, к методам и методикам измерений в процессе контроля эффективности мероприятий по ЗИ;

− установление требований к метрологическому, информационному и другим видам обеспечения ЗИ.

Система стандартов по защите информации включает следующие виды документов в области стандартизации по ЗИ, используемых на территории Российской Федерации:

− национальные стандарты Российской Федерации, в том числе ограниченного распространения, государственные военные стандарты, национальные стандарты, оформленные на основе аутентичных переводов международных стандартов (гармонизированные стандарты);

− межгосударственные стандарты;

− правила стандартизации, нормы и рекомендации в области стандартизации;

− общероссийские классификаторы технико-экономической и социальной информации;

− стандарты организаций;

− предварительные национальные стандарты

Методические рекомендации по выполнению практического занятия

ПОРЯДОК ВЫПОЛНЕНИЯ

1. Найти в открытых источника [текст ГОСТ Р ИСО/МЭК 17799-2005«Информационная технология. ПРАКТИЧЕСКИЕ ПРАВИЛА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ISO/IEC 17799:2000» (сокращенно ГОСТ Р ИСО/МЭК 17799)
2. Дать его краткую характеристику (включить в отчет).
3. Определить и описать взаимосвязь ГОСТ Р ИСО/МЭК 17799-2005 со стандартами ГОСТ Р ИСО/МЭК 27001-2006, ГОСТ Р ИСО/МЭК 27002-2012
4. В соответствие со своим вариантом дать характеристику анализируемому направлению обеспечения ИБ.
5. Сформировать требования, позволяющие проводить по ним проверку выполнения на основании трех выше указанных стандарта, оценить их важность в предлагаемой вами форме.
6. Разработайте процедуру внедрения механизмов, реализующих сформированные вами требования.
7. Разработайте подход к проверке выполнения требований, предложенных

Содержание отчета о практическом занятии

В отчете следует указать:

1. Цель работы;
2. Результат выполнение индивидуального задания;
3. Ответы на контрольные вопросы;
4. Выводы по проделанной работе.
5. Библиография

По результатам выполнения практического занятия студенты оформляют и защищают в индивидуальном порядке в форме беседы результаты выполнения заданий.

ВЫПОЛНЕНИЕ ИНДИВИДУАЛЬНОГО ЗАДАНИЯ

1. Политика безопасности
2. Организационные вопросы безопасности
3. Классификация и управление активами
4. Вопросы безопасности, связанные с персоналом
5. Физическая защита и защита от воздействий окружающей среды
6. Управление передачей данных и операционной деятельностью
7. Контроль доступа
8. Разработка и обслуживание систем
9. Управление непрерывностью бизнеса
10. Соответствие требованиям

При размещении в отчете заимственного материала следует делать соответствующие ссылки на источники.

Рекомендуемая литература

Основная литература:

1. Аверченков В.И. Служба защиты информации: организация и управления: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов - 4-е изд., стер. - Москва: ФЛИНТА, 2021. - 186 с. - ISBN 978-5-9765-1271-9. - Текст: электронный

2. Аверченков В.И. Защита персональных данных в организации: монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 4-е изд., стер. - Москва: ФЛИНТА, 2021. - 124 с. - ISBN 978-5-9765-1273-3. - Текст: электронный

3. Полякова Т.А., Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва: Издательство Юрайт, 2022. – 325 с. – (Высшее образование). – ISBN 978-5-534-03600-8.

Дополнительная литература:

1. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для. студ. учреждений сред. проф. образования / Е. Б. Белов, В. Н. Пржегорлинский. М.: Издательский центр «Академия», 2017. -336 с.

2. Солодянников А.В. Международные и российские акты и стандарты по информационной безопасности: учебное пособие / А.В. Солодянников. – СПб.: Изд-во СПбГЭУ, 2017. – 87 с.

3. Рагозин Ю.Н., Мельник В.А. Организация и управление подразделением защиты информации на предприятии: Учебное пособие / Ю.Н. Рагозин, В.А. Мельник – СПб: Издательский центр «Интермедия», 2019. – 240 с.

4. Ковалева Н.Н. Информационное право: учебник для вузов / Н.Н. Ковалева [и др.]; под редакцией Н. Н. Ковалевой. – Москва: Издательство Юрайт, 2022. – 353 с. – (Высшее образование). – ISBN 978-5-534-13786-6.

5. Аверченков В.И. Аудит информационной безопасности: учеб. пособие для вузов / В.И. Аверченков - 4-е изд., стер. - Москва: ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. - Текст: электронный

Интернет – ресурсы:

1. Официальный сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/

2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/

3. Официальный сайт Федерального агентства по техническому регулированию и метрологии (Росстандарт). – URL: http://www.gost.ru/wps/portal/.

4. Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.ru/

5. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции http://www.consultant.ru/

6. Интернет портал Защита-информации.SU http://www.iso27000.ru/
7. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru
8. Консорциум сетевых электронных библиотек ЭБС «Лань» https://e.lanbook.com/
9. ЭБС «Университетская библиотека ОНЛАЙН» https://www.biblioclub.ru/ -
10. ЭБС IPR SMART https://www.iprbookshop.ru/
11. ЭБС Znanium https://znanium.com/
12. ЭБС «Юрайт» http://www.biblio-online.ru
13. Поисковые интернет-системы Яндекс, Rambler, Google и др.

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕУЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Организационно-правовое обеспечение информационной безопасности»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль):
«Информационная безопасность киберфизических систем

Ставрополь, 2026 г.

СОДЕРЖАНИЕ

Введение

Целью освоения дисциплины «Организационно-правовое обеспечение информационной безопасности» является формирование профессиональной компетенции будущего магистра по направлению подготовки 10.04.01 «Информационная безопасность», направленность (профиль) «Информационная безопасность киберфизических систем» для осуществления деятельности в области защиты киберфизических систем, а также создания новых объектов киберфизических систем, а также теоретическая и практическая подготовленность магистра для проведения работ по обеспечению организационной и правовой безопасности информации в соответствии с современными требованиями.

Основными задачами дисциплины является:

– изучение основ правового регулирования отношений в информационной сфере, конституционных гарантий прав граждан на получение информации и механизмы их реализации;

– изучение основных понятий и видов защищаемой информации, согласно законодательству РФ;

– изучение основ правового регулирования отношений в области государственной тайны, конфиденциальной информации и интеллектуальной собственности, методов и способов защиты такой информации;

– изучение сущности и содержания организационных мероприятий по защите информации;

– обучение студентов основам расследования преступлений в информационной и компьютерной сферах;

– приобретение студентами знаний, умений и практических навыков по правовому и организационному обеспечению защиты информации.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ПК-3 Способен разрабатывать предложения по совершенствованию системы управления информационной безопасностью киберфизических систем	ИД-1 ПК-3 Демонстрирует понимание структуры и функций организационно‑управленческого аппарата системы управления информационной безопасностью	Классифицирует защищаемую информацию по видам тайны и уровням конфиденциальности Разрабатывает нормативные документы и регламенты по совершенствованию системы управления информационной безопасностью Внедряет средства защиты информации в инфраструктуру киберфизических систем

	ИД-2 ПК-3 Обеспечивает комплексную защиту информации в киберфизических системах	Оценивает уровень защищенности киберфизических систем Формирует комплекс мер по защите информации в киберфизических системах и оценивает их эффективность на основе заданных требований по безопасности информации Проектирует системы защиты информации для киберфизических систем

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные, практические занятия и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области управления информационной безопасностью. На лабораторных занятиях формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным занятиям и тестовые задания, завести новую тетрадь для конспектирования лекций и выполнения практических заданий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы студентов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к лабораторным и практическим занятиям, оформление отчета по выполненному лабораторной работе и подготовка к собеседованию по результатам работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

– чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;

– работа с нормативными документами;

– поиск информации в Интернет;

2) для закрепления и систематизации знаний:

– работа с конспектом лекции (обработка текста);

– повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);

– составление плана и тезисов ответа или графическое изображение структуры ответа;

– составление таблиц для систематизации учебного материала;

– изучение нормативных документов;

– ответы на контрольные вопросы;

3) для формирования умений:

– подготовка к лабораторным занятиям;

– решение задач и практических заданий;

– подготовка отчетов по лабораторным занятиям;

– рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические занятия, контрольные вопросы) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным занятиям.

2. Технологическая карта самостоятельной работы обучающихся дисциплине «Организационно-правовое обеспечение информационной безопасности»

Коды реализуемых копетенций, индикаторов	Вид деятельности студентов	Средства и технологии оценки	Обьем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
1 семестр					
ИД-1$_{ПК-3}$ ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$	Подготовка к практической работе	Собеседование	16.00	2.00	18.00

ИД-2$_{ПК-3}$ ИД-3$_{ПК-3}$ ИД-4$_{ПК-3}$	Подготовка к экзамену	Вопросы к экзамену	52.00	2.00	54.00
Итого за 1 семестр			68.00	4.00	72.00
Итого			68.00	4.00	72.00

3. Контрольные точки и виды отчетности по ним

По дисциплине предусмотрен текущий контроль на каждом учебном занятии и по каждому разделу учебной дисциплины.

Формы текущего контроля:

– устный опрос;

– защита отчетов по практическим занятиям.

Устный опрос осуществляется на каждом учебном занятии (лекции, практические занятия). Все практические занятия, выполняемые по разделам дисциплины, подлежат оцениванию по результатам проверки отчета и собеседованию.

Критерии оценки для проверки умений при выполнении лабораторных заданий:

– оценка «отлично» выставляется, если студент продемонстрировал высокое умение применять полученные знания на практике через решение конкретной задачи, свободно без затруднений справился с поставленной задачей, показав владение разносторонними приемами и навыками ее выполнения, не допустил ошибок и неточностей;

– оценка «хорошо» выставляется, если студент продемонстрировал умение применять полученные знания на практике через решение конкретной задачи, справился с поставленной задачей, показав владение необходимыми приемами и навыками ее выполнения, при этом допустил не более одной ошибки;

– оценка «удовлетворительно» выставляется, если студент продемонстрировал посредственное умение применять полученные знания на практике через решение конкретной задачи, с трудом справился с поставленной задачей, при этом допустил не более двух ошибок;

– оценка «неудовлетворительно» выставляется, если студент не продемонстрировал умение применять полученные знания на практике через решение конкретной задачи, не справился с поставленной задачей или допустил при ее решении три и более серьезные ошибки.

4. Методические указания по подготовке к практическим занятиям

При подготовке к практической работе студенту следует:

– изучить (повторить) теоретический материал, посвящённый теме практического занятия;

– ознакомиться с заданием на практическую работу;

– проверить свой уровень подготовки с помощью вопросов и заданий для самоконтроля.

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ:

– ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;

– убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;

– включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы:

– выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторной работе;

– подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

– при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы:

– доложить руководителю занятий или лаборанту о завершении работ.

– привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

По результатам выполнения практической работы студенты оформляют и защищают в индивидуальном порядке в форме собеседования результаты выполнения заданий.

При подготовке и выполнении практических работ совместно с оформлением отчетов по практическим занятиям позволяет успешно овладеть умениями, необходимыми для дальнейшей учебной и профессиональной деятельности.

5. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Вопросы к экзамену (1 семестр)

Вопросы (задача, задание) для проверки уровня обученности «Знать»

1. Государственная система защиты информации в Российской Федерации, ее организационная структура и функции
2. Элементы государственной системы защиты информации в Российской Федерации. Федеральная служба безопасности
3. Элементы государственной системы защиты информации в Российской Федерации. Федеральная служба по техническому и экспортному контролю
4. Основные принципы и условия организационной защиты информации
5. Основные подходы и требования к организации системы защиты информации
6. Основные силы и средства, используемые для организации защиты информации
7. Цели и задачи организационной защиты информации, ее связь с правовой и инженерно-технической защитой информации
8. Основные направления, принципы и условия организационной защиты информации
9. Угрозы информационной безопасности объекта
10. Организационные источники и каналы утечки информации
11. Модели нарушителей информационной безопасности на объекте
12. Основные функции, задачи и особенности службы безопасности объекта
13. Принципы организации службы безопасности объекта
14. Типовая структура службы безопасности
15. Основные документы, регламентирующие деятельность службы безопасности объекта
16. Основные функции службы безопасности объекта
17. Способы и формы участия сотрудников в организационной защите информации
18. Способы и формы взаимодействия службы безопасности объекта с контрразведывательными и правоохранительными органами
19. Подразделения службы безопасности объекта
20. Виды и способы охраны
21. Организация пропускного и внутриобъектового режима
22. Требования к помещениям, в которых циркулирует защищаемая информация
23. Пропуск сотрудников, посетителей на объект и в выделенные (категорированные) помещения. обеспечение режима в выделенных помещениях

24. Специальные технические средства охраны. охрана периметра
25. Технические средства видеонаблюдения объекта
26. Оружие, используемое для охраны объектов. индивидуальная защита от оружия нападения
27. Противопожарная охрана
28. Общие положения организации контрольно-пропускного режима
29. Подготовка исходных данных для разработки контрольно-пропускного режима. разработка инструкции о пропускном режиме
30. Атрибутные и биометрические идентификаторы людей. виды пропусков
31. Оборудование КПП. порядок вывоза/выноса, ввоза/вывоза материальных ценностей и документации на/с территории организации
32. Развитие права в сфере информационной безопасности
33. Предмет информационного права в информационной безопасности
34. Общая характеристика законодательства Российской Федерации в области информационной безопасности
35. Правовое обеспечение защиты государственной тайны
36. Система защиты государственной тайны
37. Правовое обеспечение защиты банковской, профессиональной и служебной тайны
38. Правовое обеспечение защиты коммерческой тайны
39. Правовое обеспечение защиты персональных данных
40. Правовое обеспечение защиты интеллектуальной собственности
41. Правовая охрана и защита патентного и авторского права
42. Документы Гостехкомиссии России. Единые критерии, стандарты. Общая характеристика «Руководящих документов Гостехкомиссии России»
43. Общие сведения об «Единых критериях безопасности информационных технологий» и ГОСТ Р ИСО\МЭК 15408
44. Характеристика основных положений «Единых критериев»
45. Анализ требований безопасности компонентов автоматизированных систем в рамках «Единых критериев»
46. Понятие компьютерных преступлений и их классификация
47. Способы совершения компьютерных преступлений
48. Раскрытие понятий, виды и элементы состава преступления
49. Характеристика международного и российского законодательства в сфере информации, информатизации и защиты информации
50. Уголовно-правовая характеристика преступлений в сфере компьютерной информации
51. Классификация компьютерных преступлений
52. Криминалистическая характеристика преступлений в сфере компьютерной информации
53. Возможности использования специальных познаний в ходе расследования преступлений в сфере компьютерной информации
54. Виды судебных экспертиз, проводимых по делам о преступлениях в сфере компьютерной информации
55. Задачи, решаемые в ходе компьютерных экспертиз
56. Административная ответственность за правонарушения в сфере информационной безопасности

57. Уголовная ответственность за правонарушения в сфере информационной безопасности

58. Выявление компьютерных преступлений

59. Методики проведения следственных действий по расследованию компьютерных преступлений

60. Общие принципы лицензирования деятельности в области защиты информации

61. Порядок лицензирования деятельности предприятий в области защиты информации, подлежащих лицензированию ФСБ России

62. Порядок лицензирования деятельности предприятий в области защиты информации, подлежащих лицензированию ФСТЭК России

63. Общие сведения о сертификации средств защиты информации

64. Положение о сертификации средств защиты информации

65. Порядок проведения сертификации средств защиты информации по требованиям безопасности информации

66. Аттестация объектов информатизации в области защиты информации

Вопросы (задача, задание) для проверки уровня обученности «Уметь, Владеть»

Задача 1

В целях ознакомления с деталями коммерческого проекта руководителем структурного подразделения компании А. через корпоративную почту на личный публичный почтовый адрес была отправлена соответствующая информация (об указанном коммерческом проекте). Факт отправления был установлен.

1. Установите значение основных понятий.
2. Какое правомерное решение может быть принято в отношении работника А.?
3. Укажите условия, при наличии которых работник может быть привлечен к ответственности.
4. Укажите виды и меры ответственности за совершенное деяние.

Задача 2

Работник IT управления компании А. в установленном порядке оформил государственную регистрацию права на программу для ЭВМ, созданную в процессе выполнения служебного задания. В суд поступил иск от директора данного управления Б. о включении его в число соавторов, поскольку он осуществлял организацию деятельности по созданию программы и непосредственное руководство работами, вносил предложения и коррективы в создаваемый продукт. Условия реализации права авторства договором не оговорены.

1. Укажите виды интеллектуальных прав на указанную в условии программу.
2. Укажите правосубъектность гражданина А., Б. и соответствующего работодателя в сфере реализации авторских прав на указанную программу.
3. Сформулируйте решение по указанному делу.
4. Сделайте выводы о том, какие действия должны быть предприняты для реализации комплекса авторских прав при условии создания соответствующего объекта.

Задача 3

Автор служебного изобретения обратился в суд с иском к организации (работодателю) о выплате вознаграждения за использование разработанного им изобретения, компенсации за невыплату вознаграждения и возмещении расходов на оплату государственной пошлины.

Патент на изобретение был выдан организации 12 сентября 2013 г. На производстве организации изобретение было внедрено 10 февраля 2010 г (действие патента прекращено 4 апреля 2020 г.) и продолжают использоваться (отдельные признаки изобретения). Авторское вознаграждение за использование изобретения не выплачивается.

1. Раскройте сущность основных понятий.
2. Раскройте особенности данного дела с указанием ссылок на соответствующие статьи.

3. Укажите условия, необходимые для принятия решения по данному делу.
4. Сформулируйте возможное решение по указанному делу.

Задача 4

Юридическое лицо обратилось в арбитражный суд с иском к индивидуальному предпринимателю о защите исключительного права на товарный знак, а также о принятии обеспечительных мер в виде запрета ответчику совершать действия по передаче домена другому регистратору.

1. Раскройте сущность основных понятий.
2. Раскройте особенности данного дела с указанием ссылок на соответствующие статьи.
3. Укажите условия, необходимые для принятия решения по данному делу.
4. Сформулируйте возможное решение по указанному делу.

Задача 5

Гражданин Б. обратился в суд с иском в отношении ряда издательств о защите интеллектуальных прав, а также взыскании компенсации за неправомерное использование его произведений и компенсации морального вреда. Указанные автором издания опубликовали и реализовали сборники, содержащие произведения, которые частично копируют сочинения истца. При этом фрагменты из сочинений истца составляют большую часть текста, положенного в основу произведений, размещенных в сборнике.

Автор посчитал, что ответчики нарушили его интеллектуальные права на созданные им произведения, реализовав сборники, содержащие фрагменты его сочинений.

1. Раскройте сущность основных понятий.
2. Укажите виды неимущественных интеллектуальных прав автора на указанные в условии произведения.
3. Укажите виды имущественных интеллектуальных прав автора на указанные в условии произведения.
4. Назовите особенности правовой защиты личных неимущественных прав.
5. Назовите особенности правовой защиты личных имущественных прав.
6. Назовите уточнения, которые могут потребоваться для решения судебного спора.
7. Сформулируйте возможное решение по указанному делу.

Рекомендуемая литература

Основная литература:

1. Аверченков В.И. Служба защиты информации: организация и управления: учеб. пособие для вузов / В.И. Аверченков, М.Ю. Рытов - 4-е изд., стер. - Москва: ФЛИНТА, 2021. - 186 с. - ISBN 978-5-9765-1271-9. - Текст: электронный

2. Аверченков В.И. Защита персональных данных в организации: монография / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин. - 4-е изд., стер. - Москва: ФЛИНТА, 2021. - 124 с. - ISBN 978-5-9765-1273-3. - Текст: электронный

3. Полякова Т.А., Стрельцов А.А. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для вузов / под редакцией Т. А. Поляковой, А. А. Стрельцова. – Москва: Издательство Юрайт, 2022. – 325 с. – (Высшее образование). – ISBN 978-5-534-03600-8.

Дополнительная литература:

1. Белов Е.Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для. студ. учреждений сред. проф. образования / Е. Б. Белов, В. Н. Пржегорлинский. М.: Издательский центр «Академия», 2017. -336 с.

2. Солодянников А.В. Международные и российские акты и стандарты по информационной безопасности: учебное пособие / А.В. Солодянников. – СПб.: Изд-во СПбГЭУ, 2017. – 87 с.

3. Рагозин Ю.Н., Мельник В.А. Организация и управление подразделением защиты информации на предприятии: Учебное пособие / Ю.Н. Рагозин, В.А. Мельник – СПб: Издательский центр «Интермедия», 2019. – 240 с.

4. Ковалева Н.Н. Информационное право: учебник для вузов / Н.Н. Ковалева [и др.]; под редакцией Н. Н. Ковалевой. – Москва: Издательство Юрайт, 2022. – 353 с. – (Высшее образование). – ISBN 978-5-534-13786-6.

5. Аверченков В.И. Аудит информационной безопасности: учеб. пособие для вузов / В.И. Аверченков - 4-е изд., стер. - Москва: ФЛИНТА, 2021. - 269 с. - ISBN 978-5-9765-1256-6. - Текст: электронный

Интернет – ресурсы:

1. Официальный сайт Федеральной службы по техническому и экспортному контролю https://fstec.ru/

2. Официальный сайт Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) https://rkn.gov.ru/

3. Официальный сайт Федерального агентства по техническому регулированию и метрологии (Росстандарт). – URL: http://www.gost.ru/wps/portal/.

4. Официальный сайт Федеральной службы безопасности Российской Федерации http://www.fsb.ru/

5. Консультант Плюс - законодательство РФ кодексы и законы в последней редакции http://www.consultant.ru/

6. Интернет портал Защита-информации.SU http://www.iso27000.ru/
7. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru
8. Консорциум сетевых электронных библиотек ЭБС «Лань» https://e.lanbook.com/
9. ЭБС «Университетская библиотека ОНЛАЙН» https://www.biblioclub.ru/ -
10. ЭБС IPR SMART https://www.iprbookshop.ru/
11. ЭБС Znanium https://znanium.com/
12. ЭБС «Юрайт» http://www.biblio-online.ru
13. Поисковые интернет-системы Яндекс, Rambler, Google и др.