*ВЕСТНИК ВОЕННОГО ИННОВАЦИОННОГО ТЕХНОПОЛИСА «ЭРА», 2022, том 3, № 4, с. 392–400*

## ЭЛЕКТРОННАЯ КОМПОНЕНТНАЯ БАЗА И ИНТЕЛЛЕКТУАЛЬНЫЕ СИСТЕМЫ УПРАВЛЕНИЯ

*УДК 004.056*

# МОНИТОРИНГ СОБЫТИЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ТЕХНОЛОГИИ И МЕТОДЫ КОНТРОЛЯ ЭФФЕКТИВНОСТИ

**© 2022 г. А. В. Дорофеев[1], А. С. Марков[1,*]**

[1] *АО "Эшелон", Москва, Россия*

******E-mail: a.markov@npo-echelon.ru*

Поступила в редакцию 15.03.2022 г.
После доработки 20.03.2022 г.
Принята к публикации 20.03.2022 г.

Показано применение современных подходов к организации мониторинга событий информационной безопасности (ИБ) на примере отечественной системы управления событиями ИБ KOMRAD Enterprise SIEM, а также возможное проведение киберучений для контроля эффективности мониторинга ИБ. Показаны таксономии, на базе которых формируются сценарии киберучений. Представлено краткое сравнение таксономии MITREATT&CK и методического документа ФСТЭК России по оценке угроз ИБ. Продемонстрирована возможность применения российских методических документов ФСТЭК России для разработки сценариев киберучений. Сделан вывод, что киберучения позволяют осуществлять эффективный контроль организации мониторинга ИБ.

**DOI:** 10.56304/S2782375X22040052

## ВВЕДЕНИЕ

Мониторинг событий информационной безопасности (**ИБ**) представляет собой сбор и анализ событий ИБ для выявления потенциальных инцидентов ИБ [1–3]. Требования по организации мониторинга ИБ предъявляются к ГИС, ИСПДн, КИИ, АСУ ТП и другим системам. В настоящее время данная задача эффективно может быть решена только с помощью автоматизации процесса и применения информацицонных систем класса **SIEM** (*Security Information and Event Management*). Данные системы на российском рынке информационной безопасности появились несколько лет назад сначала в виде западных решений, а позже и в виде отечественных разработок. До недавнего времени применение SIEM-систем оставалось прерогативой исключительно крупных организаций, которые могли себе позволить штат экспертов-аналитиков и серьезные вложения в программное и аппаратное обеспечение [3, 4]. Сейчас рынок SIEM-систем переживает трансформацию в связи с появлением решений, которые могут себе позволить и небольшие организации с довольно ограниченными ресурсами.

Приобретение и первоначальная настройка SIEM-системы являются первыми шагами для организации действительно эффективного мониторинга ИБ, за которыми обязательно должны следовать регулярный контроль эффективности работы системы и постоянное обучение специалистов по кибербезопасности, ответственных за своевременное выявление инцидентов и реагирование на них. Организовать такой контроль позволяет проведение регулярных киберучений.

## СОВРЕМЕННАЯ КИБЕРАТАКА И МЕТОДЫ ЕЕ ФИКСАЦИИ

Кратко рассмотрим, что из себя представляет современная целенаправленная кибератака [5–8]. Современная кибератака хорошо структурируется и позволяет выделить определенные этапы. Все начинается со сбора данных о цели, так называемой рекогносцировки. Злоумышленники определяют доменные имена, IP-адреса, имена учетных записей пользователей, версии программного обеспечения (**ПО**) и т.п. После этого происходит подготовка к нападению и выбирается вектор атаки – наиболее эффективный и наименее трудозатратный способ проникновения в сеть. Они могут взламывать как сетевые сервисы, доступные из интернет, так и атаковать пользователей, отправляя им письма, содержащие вредоносные вложения либо ссылки на них. После того как злоумышленники оказались в инфраструктуре, их основной задачей становится организация комфортного удаленного доступа к скомпрометированной сети. Для этого они используют имеющиеся учетные записи (скомпрометированные), либо создают свои, либо используют возможности вредоносного ПО, которое устанавливает скрытую связь с серверами управления, контролируемым злоумышленниками. Затем

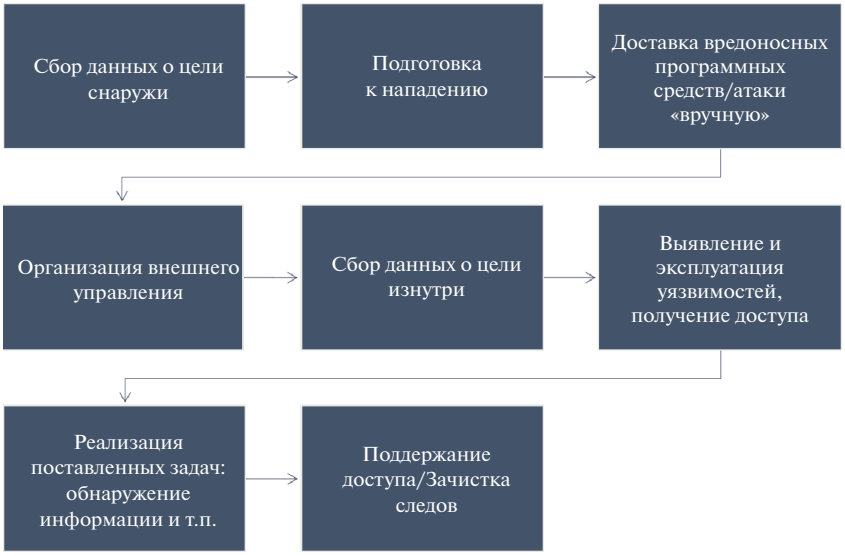


**Рис. 1.** Ключевые этапы целенаправленной атаки.

злоумышленникам необходимо собрать данные о других целях, доступных уже изнутри. Они находят почтовые и файловые серверы, контроллеры доменов, базы данных, рабочие станции администраторов и руководителей организации. Собирают информацию о типах и версиях сервисов, которая позволит выявить уязвимости и провести их эксплуатацию. Получив полный контроль над инфраструктурой, злоумышленники осуществляют те задачи, которые были перед ними поставлены до проникновения. Криминальные хакерские группы заинтересованы в первую очередь в получении финансовых средств, соответственно, их будут интересовать данные, которые можно продать, либо данные, которые можно использовать для последующего вымогательства денег, зашифровав их, либо угрожая их опубликовать. Злоумышленники могут и просто украсть деньги, если они получат доступ к системам, через которые возможны манипуляции с денежными средствами на счетах организации или ее клиентов (если организация – банк). Если злоумышленники являются представителями спецслужб иностранных государств, то их скорее всего заинтересует получение либо определенной информации, либо организация постоянного присутствия в инфраструктуре для того, чтобы в нужный момент можно было осуществить акт саботажа, отключив критичный ресурс или вмешавшись в технологический процесс. В зависимости от мотивации злоумышленников по-разному будут выглядеть и заключительные этапы атаки. В случае криминала злоумышленники постараются максимально уничтожить следы своего присутствия и затруднить расследование. В случае спецслужб они постараются организовать незаметный доступ (рис. 1).

Существуют несколько известных подходов к структурированному описанию действий злоумышленников, предпринимаемых в ходе кибератаки [9, 10]. До недавнего времени наиболее цитируемой в литературе являлась семиэтапная модель Cyber Kill Chain. Более современным подходом является применение матрицы MITRE ATT&CK, которая включает в себя 14 так называемых “тактик”, представляющих собой целевые задачи и 144 “техники” – конкретных действий злоумышленников.

Методика оценки угроз ИБ, разработанной ФСТЭК России, включает в себя 10 целевых задач:

Т1. Сбор информации;

Т2. Получение первоначального доступа;

Т3. Внедрение и исполнение вредоносного ПО;

Т4. Закрепление доступа;

Т5. Управление вредоносным ПО;

Т6. Повышение привилегий;

Т7. Сокрытие действий;

Т8. Распространение доступа к смежным системам;

Т9. Сбор и вывод из системы информации,

Т10. Несанкционированное воздействие или доступ (целевое воздействие).

Указанные целевые этапы включают в себя 145 описаний конкретных действий злоумышленников. Несложно сравнить указанный подход с систематикой ATT&CK. Из-за ограничений в

**Таблица 1.** Пример сравнения целевых задач по ФСТЭК России и MITREATT&CK

| Т4. Закрепление доступа | |
|---|---|
| ID ФСТЭК России | MITRE ATT@CK |
| Т4.1. Несанкционированное создание учетных записей | T1136<br>T1212 |
| Т4.2. Использование штатных средств удаленного доступа ОС | T1133<br>T1021 |
| Т4.3. Скрытая установка и запуск средств удаленного доступа ОС | T1133<br>T1021<br>T1219 |
| Т4.4. Маскирование подключенных устройств под легитимные | близко к T1036 |
| Т4.5. Внесение соответствующих записей в компоненты автозапуска | T1542<br>T1053<br>T1547<br>T1037 |
| Т4.6. Компрометация прошивок устройств | T1542.001<br>T1495 |
| Т4.7. Резервное копирование вредоносного кода в скрытые области | отсутствует |

объеме публикации ограничимся сравнением одного целевого этапа (“тактики”) Т4 (табл. 1) [9, 11].

Применение подобных классификаций позволяет не только описывать хакерские атаки, возможности вредоносного ПО, но и планировать сценарии киберучений, а также оценивать полноту покрытия хакерских действий правилами средств защиты информации SIEM, IDS и др.

## ПРИНЦИПЫ И ТЕХНОЛОГИИ РАБОТЫ SIEM-СИСТЕМ

Разберем принципы работы SIEM-систем на примере сертифицированного отечественного продукта KOMRADEnterpriseSIEM, разработанного АО “НПО “Эшелон”.

SIEM-система должна позволять получать события из источников, приводить к единому формату и позволять фильтровать только критичные события, а также выявлять потенциальные инциденты на основе срабатывания правил корреляции, позволяющих задать цепочку событий с определенными условиями по времени регистрации и данным событий и т.п. (рис. 2). В случае регистрации инцидента осуществляется уведомление ответственных специалистов, а также возможно автоматическое реагирование (запуск скрипта реакции).

События ИБ могут поступать в KOMRAD Enterprise SIEM из различных источников: ОС, СУБД, сетевого оборудования, СЗИ, прикладного ПО и т.д. Для сбора событий используются коллекторы. Некоторые из них работают в пассивном режиме, ожидая входящих данных на заданных сетевых портах (*Syslog*, *xFlow*), другие сами инициируют соединения для извлечения необходимой информации (SQL, файловый, SNMP). Для сбора событий с Windows-машин используется специальный WMI-агент.

Коллекторы могут быть установлены как на одном узле с основными компонентами системы, так и на выделенных серверах.

Важнейшими коллекторами, которые позволяют организовать сбор событий с абсолютного большинства источников, являются Syslog-коллектор и сбор с Windows-машин с помощью WMI-агента.

Подключение источника для передачи событий по Syslog заключается во включении Syslog-коллектора и настройке источника для передачи событий на определенный порт и IP-адрес.

Для Syslog-коллектора можно установить параметры пропускной способности, ограничивающие число одновременных соединений, а также


**Рис. 2.** Принцип работы SIEM-системы.

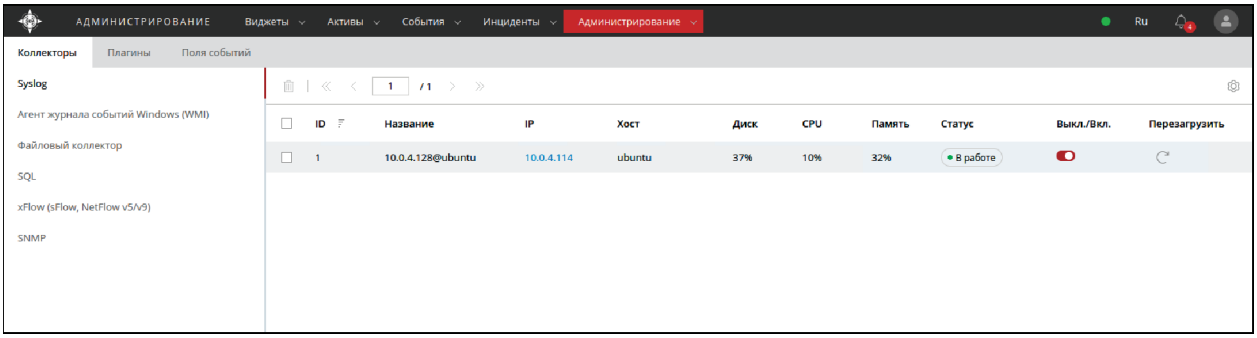


**Рис. 3.** Управление Syslog-коллекторами.

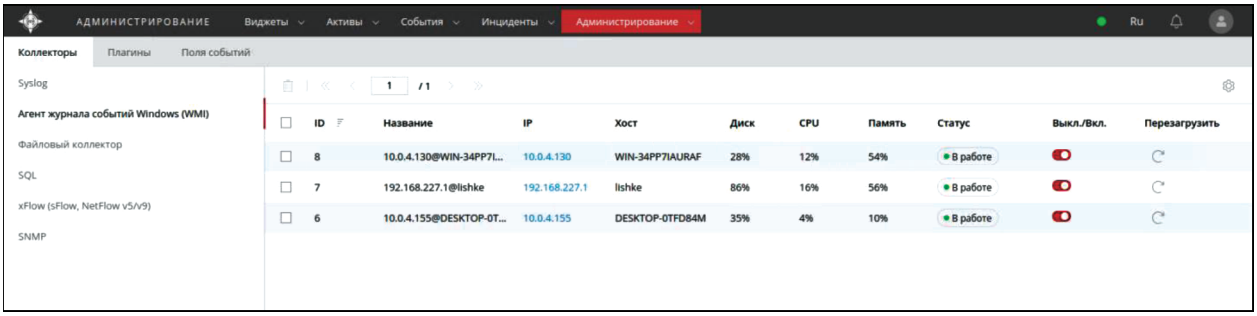


**Рис. 4.** Управление WMI-агентами.

размер входящих сообщений передачи на слабых каналах связи (рис. 3).

Подключение Windows-машины в качестве источника событий доступно для администраторов системы за три простых шага, а именно: одной командой установить агент на нужный узел, в конфигурационном файле указать IP-адрес коллектора KOMRAD Enterprise SIEM, после чего применить настройки.

WMI-агент также позволяет собирать данные из локальных файлов журналов. Агенты устанавливаются в качестве службы Windows и управляются через веб-интерфейс администратора KOMRAD Enterprise SIEM (рис. 4).

После подключения источников событий в системе можно наблюдать за потоком поступающих событий (рис. 5).

Для того чтобы можно было осуществлять с данными поступающих событий различные манипуляции (сравнивать с помощью фильтров по заданным значениям, извлекать данные в директивах корреляции), необходимо их разобрать на составляющие поля – нормализовать.

В случае если событие приходит через коллектор, для которого не установлен плагин нормализации либо под данный тип событий отсутствует подходящий плагин или регулярное выражение, то автоматически заполняются лишь поля внутренней структуры события KOMRAD Enterprise SIEM (встроенные поля). Некоторые поля событий для коллекторов WMI и SQL (SQL.TaskName) генерируются только при получении события ИБ, для остальных коллекторов набор полей реализуется через Elastic Common Schema (ECS). Если источник событий передает события в формате CEF (Common Event Format), RFC 3164, RFC 5424, то поля событий будут автоматически нормализованы. Также в KOMRAD Enterprise SIEM имеется возможность создания пользовательских полей событий.

После того как события были получены от источника и прошли процесс нормализации, они попадают в хранилище и коррелятор. Для выбора событий, соответствующих необходимым критериям, используются фильтры (запросы), которые можно формировать с помощью графического конструктора, автоматически преобразующего блоки конструктора в выражение для поиска событий по поставленным условиям, либо сразу на языке Lua.

Фильтры очень гибкие и представляют собой условия, объединенные между собой логическими операторами И/ИЛИ. В условиях может быть использовано множество различных операторов сравнения, например: “равно”, “не равно”, “содержит”, “не содержит”, “начинается с”, “не начинается с”, “содержит примерно” и т.п. (рис. 6).

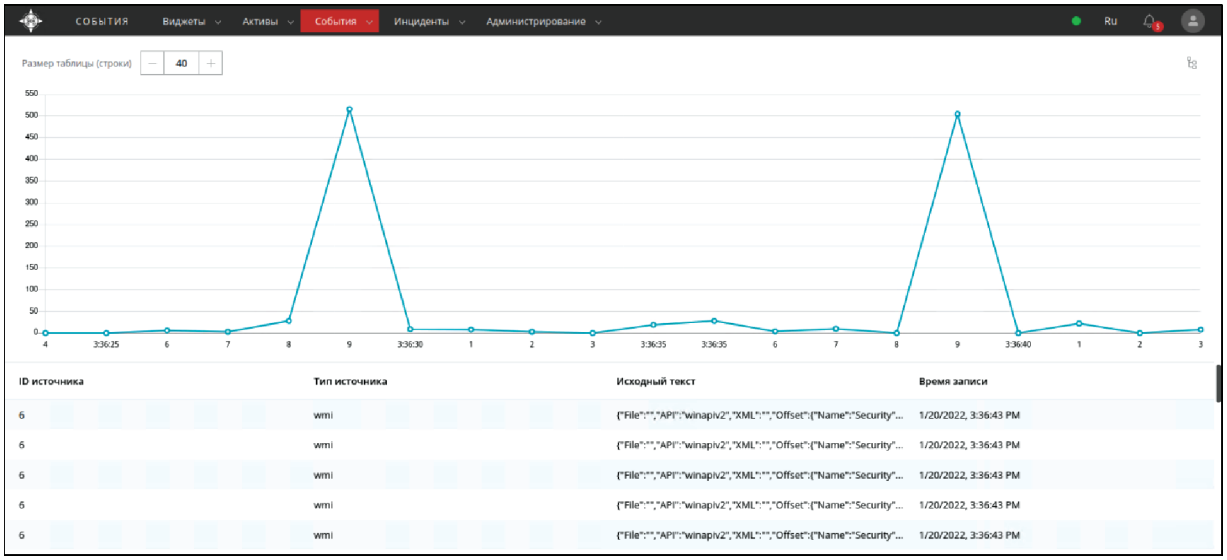


**Рис. 5.** События в реальном времени.

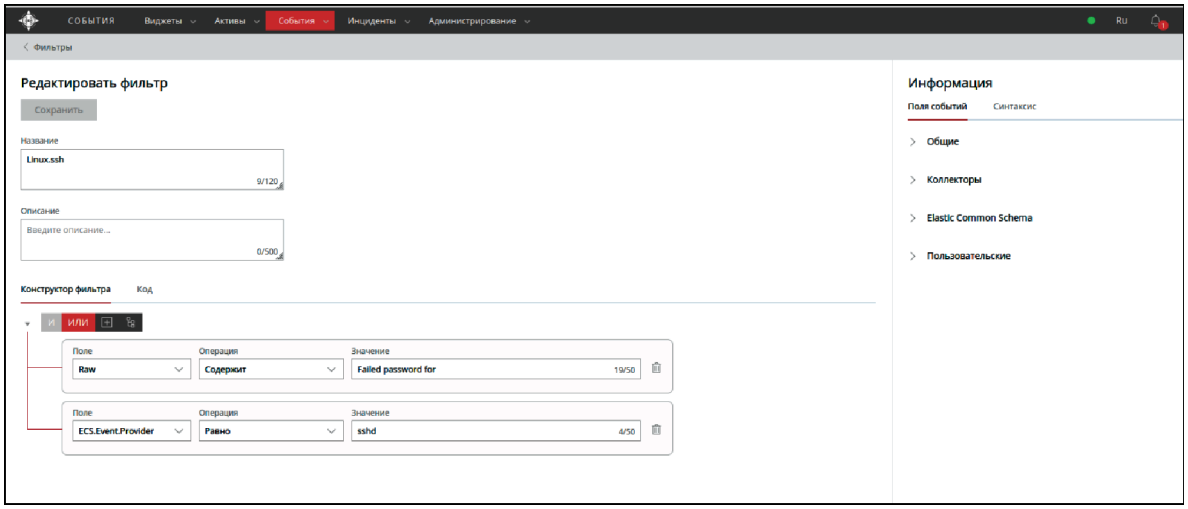


**Рис. 6.** Пример фильтра.

Состав полей фильтра задает индексируемые поля событий, по которым возможен быстрый поиск. Фильтры являются основой для формирования директив корреляции.

Корреляция данных – сравнение параметров данных о событиях ИБ с заданными граничными показателями для выявления инцидентов ИБ. Директива корреляции представляет собой логическую совокупность правил, построенную по иерархическому принципу, в соответствии с которыми осуществляется сравнение параметров событий ИБ, а также их количества и частоты с заданными показателями для выявления инцидентов ИБ.

В KOMRAD Enterprise SIEM существует собственный графический конструктор для управления директивами корреляции (рис. 7).

В случае срабатывания директивы корреляции в интерфейсе пользователя появляется уведомление об инциденте. Уведомление также можно направить по e-mail, если ресурсы организации не позволяют постоянный контроль за работой системы со стороны специалистов ИБ.

## МЕТОДИЧЕСКИЕ ОСНОВЫ КИБЕРУЧЕНИЙ

В настоящее время терминологический аппарат киберучений находится на стадии становления, и истоки его лежат в военной области [9, 11–

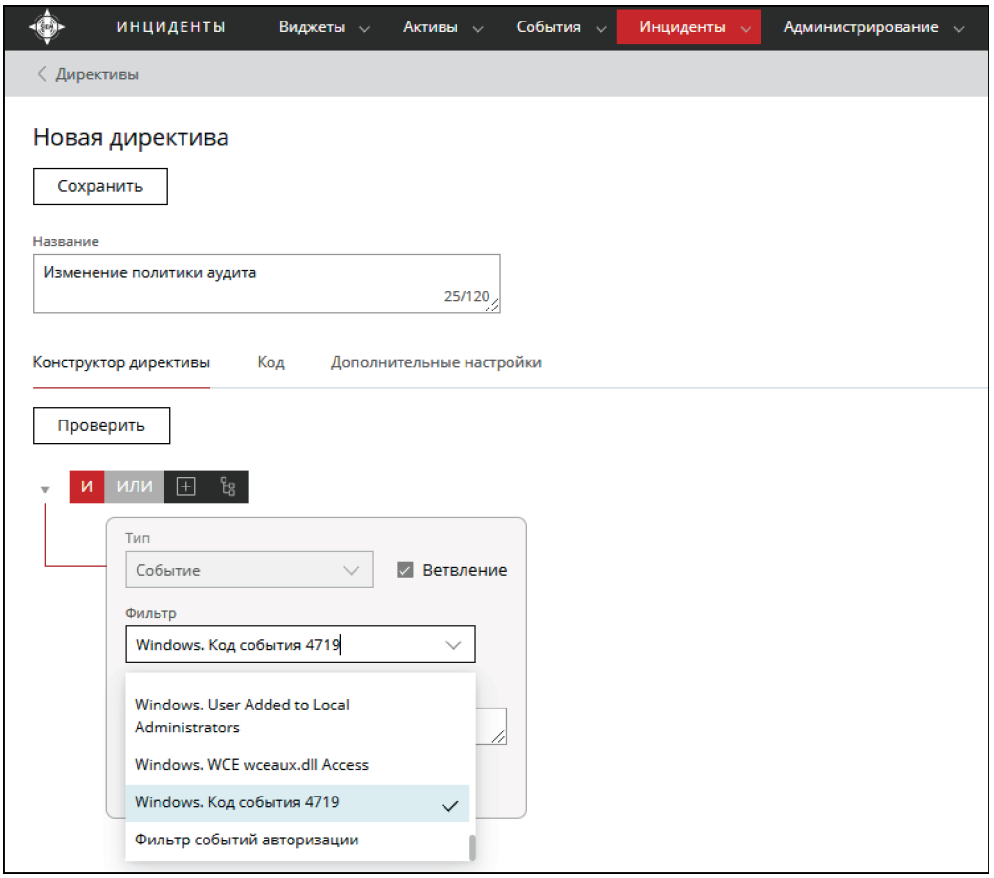


**Рис. 7.** Графический конструктор.

16]. Так, MITRE Cyber Exercise Playbook практически относит учения к имитации военной кибероперации (включающей планирование, подготовку и выполнение), которая проводится с целью обучения и оценки организации с упором на программу обеспечения ИБ. В документе NIST SP 800-84 (Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities) отмечается, что учения должны представлять имитацию чрезвычайной ситуации, разработанной для проверки плана ИТ, в первую очередь ролей и обязанностей персонала. Исследования МСЭ по кибербезопасности трактуют цели киберучения как совершенствование скоординированных действий по реагированию на инциденты в компьютерной сфере в вопросах борьбы с киберугрозами. Согласно ISO 22398 (Guidelines for Exercises) учения могут использоваться для проверки документов, обучения, уточнения и обучения персонала ролям и обязанностям, улучшения координации и коммуникаций, улучшения индивидуальных показателей и пр. Что касается перспективного стандарта ISO/IECTR 27109 (Cybersecurity Education and Training), то термин там пока не состоялся.

Развернутое определение дано в документе Европейской организации по кибербезопасности – ECSO, где киберучения трактуются как запланированное мероприятие, в ходе которого организация имитирует кибератаки, инциденты ИБ или другие виды нарушений с целью проверки киберсвозможностей организации, начиная от способности обнаружить инцидент безопасности и заканчивая способностью адекватно реагировать и минимизировать любые связанные с ним последствия.

Отметим ряд особенностей киберучений:

– проведение имитации чрезвычайной ситуации в области ИБ;

– проверка актуальных и реализуемых (а не гипотетических) угроз, уязвимостей и компьютерных атак в области ИБ;

– использование комплексной учебной программы, включающей в себя игровой сценарий, который может быть развит в процессе игры;

– совершенствование как осведомленности персонала, их ролей и обязанностей, координации действий, так и способности принимать решения в нестандартных ситуациях.

Относительно последнего пункта отметим, что обучение требует отработки принятия решений на основе полученных знаний по Расмуссену, на-

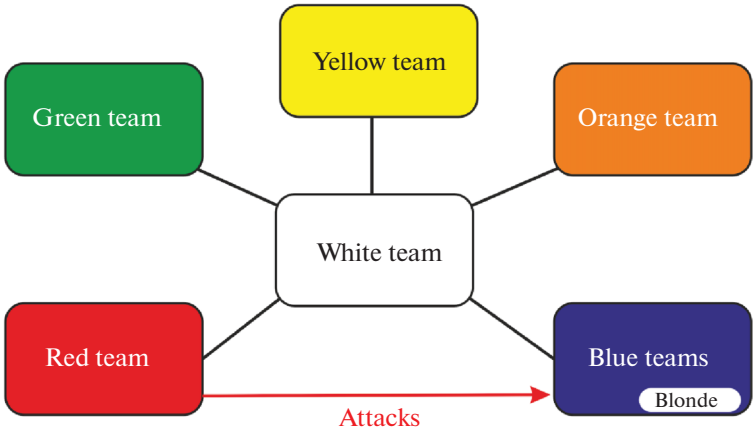


**Рис. 8.** Примеры киберкоманд.

пример в ситуации, которая не прописана в руководствах по управлению инцидентами и реагированию на компьютерные атаки.

В киберучениях задействованы как минимум две команды: нападающие (Red Team) и защищающиеся (Blue Team). В масштабных киберучениях могут быть и другие команды: Green team – администраторы, White team – организаторы, Yellow team – исследователи и пр. (рис. 8).

Задачи и ожидания от киберучений определяются конкретными целями и возможностями, например могут включать в себя следующие:

– обучить технический персонал применению средств защиты информации;

– повысить осведомленность в области кибербезопасности;

– отработать процесс принятия управленческих решений в ходе процедуры реагирования на инцидент;

– отработать процессы коммуникаций в команде защищающихся;

– проверить адекватность принятых в организации регламентов по реагированию на инциденты и т.д.

## ПРИМЕР ОРГАНИЗАЦИИ КИБЕРУЧЕНИЙ НА УЧЕБНОЙ МОДЕЛИ КОМПЬЮТЕРНОЙ СЕТИ, МОНИТОРИНГ КОТОРОЙ ОСУЩЕСТВЛЯЕТСЯ С ПОМОЩЬЮ KOMRAD ENTERPRISE SIEM

Следует сказать, что в стране существует рынок услуг по проведению киберучений. Можно отметить соответствующие среды: Ampire (“Перспективный мониторинг”), BI.ZONE Cyber Polygon, Jet CyberCamp (“Инфосистемы Джет”), The Standoff (Positive Technologies), “Киберполигон” (ООО “Киберполигон”), Национальный киберполигон и платформа “Кибермир” (“Ростелеком”) и др. В то же время УЦ “Эшелон” имеет положительный опыт организации киберучений под эгидой Минобороны России. Далее рассмотрим пример проведения киберучений в рамках курсов повышения квалификации в АНО “Учебный центр “Эшелон” на специальном киберполигоне. Киберполигон позволяет моделировать кибератаки на компьютерные сети предприятий и обучать специалистов на должном уровне. Ниже представлена схема сети киберполигона для тренинга начального уровня.

В рассматриваемой виртуальной ИТ-инфраструктуре в качестве целей используются серверы, размещенные в DMZ-сегменте, с запущенными http/ftp/ssh-сервисами и типовые рабочие станции на базе ОС Windows и Linux, размещенные в локальном сегменте сети. Компьютер атакующего создан на базе специализированного дистрибутива Kali Linux и размещен во внешнем сегменте сети. В рамках обучения начального уровня предполагается освоение базовых инструментов для проведения компьютерных атак, например фреймворк Metasploit Framework, комплекс анализа защищенности Сканер-ВС и другие актуальные утилиты. Из средств защиты информации применяются межсетевой экран Рубикон и решения, разрабатываемые НПО “Эшелон”, в частности KOMRAD Enterprise SIEM, Сканер-ВС и варианты СОВ.

В рамках обучения слушатели могут выполнять имитацию ряда типовых атак, после чего разбираются с тем, как их можно обнаружить, создав соответствующие правила для реальных SIEM-систем и СОВ. Фрагмент перечня действий, предпринимаемых командами нападающих и защищающихся, представлен ниже (табл. 2).

Следующая ступень обучения предполагает развитие киберполигона в направлении расширения набора сервисов в качестве целей атакующих

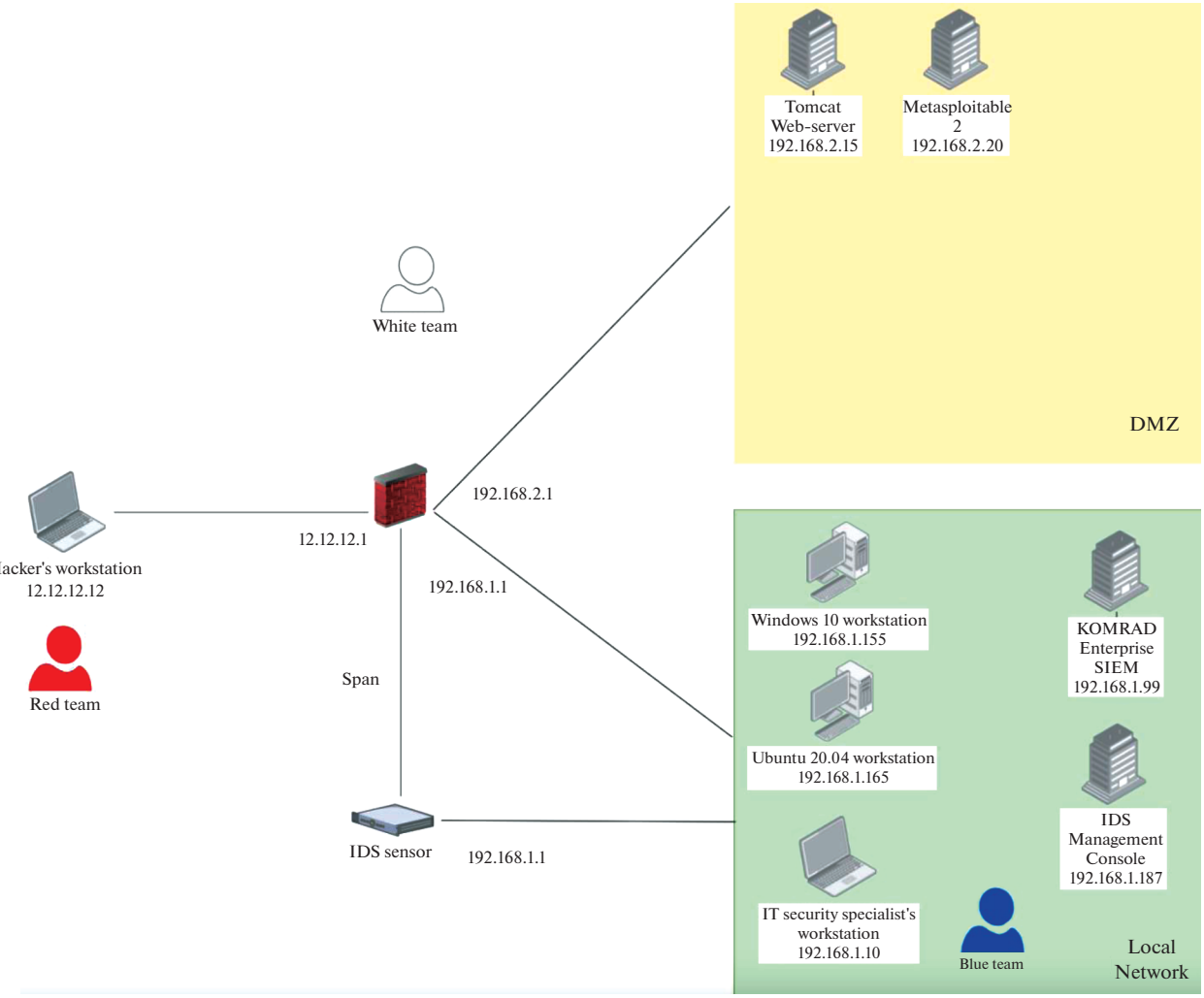


**Рис. 9.** Пример схемы киберполигона начального уровня.

(Active Directory, DNS, электронная почта, различные СУБД и т.п.), а также расширения применения инструментария нападающих (Metasploit Framework, PowerShell Empire и пр.).

## КИБЕРУЧЕНИЯ КАК СПОСОБ КОНТРОЛЯ ЭФФЕКТИВНОСТИ ОРГАНИЗАЦИИ МОНИТОРИНГА СОБЫТИЙ ИБ

В реальной инфраструктуре предприятия после развертывания и настройки SIEM-системы имеет смысл на регулярной основе проводить киберучения, отрабатывая по MITREATT@CK и методике ФСТЭК России наиболее характерные для данной ИТ-инфраструктуры сценарии атак [17–20]. Преследуемые цели включают в себя, как минимум, отладку правил СЗИ и слаживание действий специалистов по защите информации в рамках процедур реагирования на инциденты, возникающие в ходе киберучений. Очевидно, что киберучения на реальной инфраструктуре должны проводиться с рядом предосторожностей, чтобы не допустить негативного воздействия на процессы организации.

## ЗАКЛЮЧЕНИЕ

Таким образом, можно сделать ряд кратких выводов.

Мониторинг событий информационной безопасности с помощью SIEM-систем теперь доступен для организаций с ограниченными техническими и людскими ресурсами и требуется регуляторами в большинстве случаев.

В мире сложилось понимание способов структурирования и описания целенаправленных атак. Российская методологическая база в данном вопросе соответствует мировым тенденциям.

Киберучения – это актуальная форма обучения специалистов, ориентированная на реальные инциденты, а также эффективный метод контро-

**Таблица 2.** Пример настройки служб киберполигона

| № | Атака (задача Redteam) | Цели нападающего | Цель: IP | ФСТЭК | MITRE | Обнаружение (задача Blueteam) |
|---|---|---|---|---|---|---|
| 1 | Сетевая разведка | Определить сервисы, доступные для дальнейших атак | 12.12.12.1 | Т1.4 | T1595.001 | Создать правило для СОВ<br>Создать фильтр для SIEM и директиву корреляции.<br>Настроить в PFSense передачу событий по syslog в SIEM.<br>Создать плагин для PFSense для парсинга событий |
| 2 | Подбор паролей к консоли управления веб-сервером | Получение доступа к консоли управления для обеспечения возможности загрузки вредоносного ПО (ВПО) (webshell) | 192.168.2.15:8080 | Т2.10 | T1110 | Создать правило для СОВ.<br>Настроить журналирование веб-сервера tomcat.<br>Настроить rsyslog для удаленной передачи событий.<br>Создать плагин для парсинга журналов tomcat.<br>Создать директиву для определения подбора паролей по протоколу HTTP |
| 5 | Подбор паролей к хэшам из /etc/shadow | Получение учетных записей для перемещения внутри инфраструктуры | 192.168.2.15 | Т2.10 | T1110 | Настроить мониторинг auditd-доступа к файлу.<br>Настроить мониторинг передачи по сети содержимого файла.<br>Создать директиву корреляции |

ля проверки эффективности организации мониторинга информационной безопасности и корректности настройки средств защиты.

## СПИСОК ЛИТЕРАТУРЫ


1. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под ред. Зегжда Д.П. и др. М.: Горячая линия, 2021. 560 с.
2. *Петренко С.А., Ступин Д.Д.* Национальная система раннего предупреждения о компьютерном нападении. 2-е изд. СПб.: “Издательский Дом “Афина”, 2018. 448 с.
3. *Полтавцева М.А.* // Вопросы кибербезопасности. 2021. № 2 (42). С. 51.
4. *Рыболовлев Д.А., Карасёв С.В., Поляков С.А.* // Вопросы кибербезопасности. 2018. № 3 (27). С. 47.
5. *Будников С.А., Бутрик Е.Е., Соловьев С.В.* // Вопросы кибербезопасности. 2021. № 6 (46). С. 47.
6. *Васильев В.И., Кириллова А.Д., Вульфин А.М.* // Вопросы кибербезопасности. 2021. № 2 (42). С. 2.
7. *Михайлов Д.М., Дворянкин С.В., Чуманская В.В.* // Вопросы кибербезопасности. 2021. № 6 (46). С. 62.
8. *Dorofeev A.V., Markov A.S., Rautkin Y.V.* // CEUR Workshop Proceedings. V. 2522. 2019. С. 47.
9. *Дорофеев А.В., Марков А.С.* // Защита информации. Инсайд. 2022. № 2 (104). С. 56.
10. *Кондаков С.Е., Рудь И.С.* // Вопросы кибербезопасности. 2021. № 5 (45). С. 12.
11. *Dorofeev A.V., Markov A.S.* // CEUR Workshop Proceedings. 2021. V. 3057. P. 1.
12. *Бородай Р.Р., Киреев А.П., Новиков В.И., Братишко Н.М.* // Точная наука. 2019. № 66. С. 33.
13. *Бурлака И.М., Компаниец Р.И.* // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 70.
14. *Воробьев А.М., Ястребов А.В., Бирюков Д.Н.* // Методы и технические средства обеспечения безопасности информации. 2020. № 29. С. 122.
15. *Метельков А.Н.* // Правовая информатика. 2022. № 1. С. 20.
16. *Штеренберг С.И., Москальчук А.И., Коптелова В.А., Виноградова О.М.* // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Сер. 1. Естественные и технические науки. 2021. № 1. С. 32.
17. *Басан Е.С., Грицынин А.С., Шулика М.Г., Крючков В.С.* // Вопросы кибербезопасности. 2021. № 4 (44). С. 35.
18. *Макаренко С.И.* // Вопросы кибербезопасности. 2021. № 3 (43). С. 43. https://doi.org/10.21681/2311-3456-2021-3-43-57
19. *Макаренко С.И., Смирнов Г.Е.* // Вопросы кибербезопасности. 2021. № 6 (46). С. 12.
20. *Соловьев С.В., Язов Ю.К.* // Вопросы кибербезопасности. 2021. № 1 (41). С. 69.