Тема 1 Управление инцидентами информационной безопасности

Лекция 8. Центр мониторинга информационной безопасности

Дисциплина: Анализ информационных потребностей подразделений информационно-аналитического мониторинга

Доцент: Кирьянов Александр Владимирович
email:kiryanov_a@mirea.ru

Учебные вопросы и цели занятия:

1. Понятие политики информационной безопасности

2. Назначение, состав и возможности *NeuroDAT SIEM*

3. Особенности функционирования Центра мониторинга информационной безопасности NeuroDAT SIEM

Стадия реагирования на компьютерные инциденты состоит из следующих последовательных этапов:

- определение вовлеченных в компьютерный инцидент элементов информационной инфраструктуры;
- локализация компьютерного инцидента;
- выявление последствий компьютерного инцидента;
- ликвидация последствий компьютерного инцидента;
- закрытие компьютерного инцидента.

Параллельно с перечисленными действиями по реагированию на КИ могут проводиться:

- фиксация материалов, связанных с возникновением компьютерного инцидента;
- установление причин и условий возникновения компьютерного инцидента даже после закрытия компьютерного инцидента.

Выполнение данных этапов не влияет на закрытие компьютерного инцидента.

1. Понятие политики информационной безопасности

Первый учебный вопрос.

Основой ИБ организации являются четко сформулированные цели, стратегии и ПБ. Они отражают деятельность организации и обеспечивают согласованность всех защитных мер. Цели (чего необходимо достичь), стратегии (способы достижения цели), политика (правила, которые следует соблюдать при реализации стратегий) и процедуры (методы осуществления политики) могут быть определены и раскрыты как для конкретных подразделений, так и для определенного уровня иерархии организации. Цели, стратегии, политика и методы безопасности телекоммуникационных систем должны отображать то, что ожидается от нее в сфере безопасности. Как правило, их излагают на общепринятом языке, однако в некоторых случаях может возникнуть и потребность сделать это более формально, с использованием специфической терминологии. Цели, стратегия, политика определяют уровень безопасности для организации и порог приемлемого риска.

Первый учебный вопрос.

После того как организация сформулировала цели безопасности, должна быть выбрана стратегия безопасности с тем расчетом, чтобы сформировать основу для разработки ПБ.

Под политикой без опасности понимаются правила, директивы, сложившаяся практика, которые определяют, как в пределах организации и ее информационно-телекоммуникационной системы (ИТКС) управлять, защищать и распределять активы, в том числе информацию. Для разработки и эффективной реализации ПБ требуется ее организационное решение. Важно, чтобы она учитывала цели и конкретные особенности деятельности организации. В свою очередь, может возникнуть необходимость в разработке отдельной и специфической ПБ для каждой из информационной системы. Подобная политика должна быть основана на результатах анализа риска и соответствовать ПБ ИС, учитывать ее особенности.

Первый учебный вопрос.

Стратегии безопасности информационно-телекоммуникационных систем

После установления целей безопасности организации должны быть разработаны стратегии безопасности, являющиеся фундаментом развития ПБ организации. Такой подход необходим для того, чтобы гарантировать достоверность и эффективность результатов процесса управления. Для развития и успешной реализации ПБ в организации требуется обеспечить ее всестороннее управление.

Вначале рассматривается вопрос о том, насколько широки границы уровня риска, приемлемого для организации. Необходимость задания широких границ допустимого риска безопасности диктуется задачами безопасности, которые должна выполнить организация. Для решения задач по обеспечению безопасности нужно идентифицировать активы организации и провести оценку их ценности. В данном случае под активами понимается все, что имеет ценность для организации, в том числе и ИТКС.

Первый учебный вопрос.

При идентификации и определении ценности активов необходимо учитывать роль, которую они играют в поддержании деятельности организации.

Таким образом, чтобы оценить, в какой мере деятельность организации зависит от ИТКС, необходимо рассмотреть следующие вопросы:

- Какова потребность в их организации и функционировании?
- Каковы задачи, решаемые при их помощи?
- Какие важные решения зависят от конфиденциальности, целостности, доступности, неотказуемости, подотчетности и аутентичности информации, хранимой или обрабатываемой в ней, или от того, насколько эта информация актуальна?
- Какая хранимая или обрабатываемая информация должна защищаться?
- Каковы последствия инцидента безопасности?

Первый учебный вопрос.

В зависимости от целей ИБ необходимо согласовать стратегию их достижения. Так, выбранная стратегия должна соответствовать уровню ценности защищаемых активов, а ее основные положения сводятся к тому, как организация будет достигать своих целей в области ИБ. Вопросы, к которым должна обращаться стратегия, будут зависеть от числа, вида и важности этих целей. Для организации обычно важно применять типовые решения этих вопросов, характер которых может быть как конкретным, так и общим.

Другими возможными аспектами стратегии ИБ в силу специфических задач или их комбинаций могут быть:

- стратегия оценки риска и методы, адаптируемые в рамках организации;
- комплексная политика безопасности подсистем ИТКС;
- организационные методы безопасности подсистем ИТКС;
- схема классификации подсистем ИТКС;
- осознание необходимости безопасности и повышение квалификации в области безопасности;
- условия безопасности соединений, которые должны выполняться и проверяться перед осуществлением соединения с другими устройствами;
- стандартные схемы управления инцидентами информационной безопасности в рамках всей организации.

Первый учебный вопрос.

После определения стратегия безопасности и ее составляющие должны быть включены в ПБ организации. Вначале определяется, какой общий уровень риска является приемлемым для данной организации. Для того чтобы оценить и сформулировать такие цели, необходимо изучить имеющиеся активы, определить, насколько ценными они являются для данной организации и ответить на следующие вопросы:

- Какие важные элементы деятельности организации не могут осуществляться без привлечения информационных технологий?
- Какие вопросы могут решаться исключительно с помощью использования информационных технологий?
- Принятие каких важных решений зависит от достоверности, целостности или доступности информации, обрабатываемой с использованием информационных технологий, или от своевременного получения такой информации?
- Какие виды конфиденциальной информации, обрабатываемой с использованием ИТ, подлежат защите?
- Какие последствия могут наступить для организации после появления нежелательного инцидента нарушения безопасности?

Ответы на поставленные вопросы могут помочь сформулировать цели создания системы безопасности в организации, в зависимости от которых необходимо выработать стратегию их достижения, соответствующую ценности защищаемых активов. Любая стратегия, направленная на обеспечение ИБ, должна содержать общие положения о том, как организация собирается обеспечить достижение своих целей в этой области. Основное содержание этих положений стратегии будет зависеть от числа, содержания и важности поставленных целей, при этом организация обычно считает необходимым распространить поставленные требования на все свои подразделения. По своему содержанию основные положения стратегии могут иметь как специфический, так и общий характер.

В качестве других возможных основных положений стратегии безопасности, в зависимости от конкретных целей и их комбинаций, можно привести следующее:

- стратегия и методы анализа риска, используемые в масштабе всей организации;
- оценка необходимости разработки ПБ для каждой подсистемы ИТКС;
- оценка необходимости создания рабочих процедур безопасности для каждой подсистемы ИТКС;
- разработка схемы классификации подсистем ИТКС по уровню чувствительности информации в масштабах всей организации;
- оценка необходимости учета и проверка условий безопасности соединений до места подключения к ним других организаций;
- разработка схем обработки инцидентов, связанных с нарушением системы безопасности для универсального использования.

После разработки стратегии безопасности ее составные элементы должны быть включены в состав ПБ организации.

Элементы политики безопасности информационно-телекоммуникационных систем организации

Политика безопасности организации может состоять из принципов безопасности и директив для организации в целом и должна отражать более широкий круг аспектов политики организации, включая аспекты, касающиеся прав личности, законодательных требований и стандартов. Политика информационной безопасности может содержать принципы и директивы, специфичные для защиты чувствительной и ценной или важной для организации информации. Содержащиеся в ней принципы строятся на основе принципов ПБ и, таким образом, согласованы с ними.

Первый учебный вопрос.

ПБ ИТКС должна отражать существенные принципы безопасности и директивы, применимые к ПБ и политике информационной безопасности, а также порядок использования ИТКС в организации.

Наряду с этим она должна содержать особые требования по безопасности, подлежащие реализации, и процедуры правильного использования защитных мер. Политика безопасности ИТКС должна формироваться исходя из согласованных целей и стратегий безопасности организации. Необходимо выработать и сохранять ПБ, соответствующую законодательству, требованиям регулирующих органов, политике в области профессиональной деятельности, безопасности и политике ИТКС.

Еще один подход разделяет ПБ на две категории: административные, выполняемые людьми, и технические, реализуемые с помощью оборудования и программ.

Первый учебный вопрос.

Организационная (или административная) ПБ (organizational security policy) обычно излагается в документах трех уровней.

Документы верхнего уровня носят общий характер и определяют ПБ для организации в целом.

Второй уровень выделяют в случае структурной сложности организации или при необходимости обозначить специфичные области деятельности, подразделения, технологии, подсистемы и т. п.

Третий уровень относится к конкретным службам или подразделениям организации и детализирует верхние уровни ПБ. На данном уровне определяются конкретные цели, частные критерии и показатели ИБ, задаются права групп пользователей, формулируются условия доступа к информации, выводятся правила ОИБ и т. п.

Первый учебный вопрос.

Техническая ПБ (technical security policy) – это совокупность законов, правил и практических методов, регулирующих обработку чувствительной информации и использование ресурсов ПО и аппаратным обеспечением (АО) ИТКС (www.finam.ru/dictionary).

Техническая ПБ базируется на правилах двух видов: правилах разграничения доступа ко всем информационным ресурсам организации и правилах анализа сетевого трафика как внутри интранета, так и при его выходе или входе из интранета. В основе этих правил лежит принцип доверия – пользователям, приложениям, процессам, базам данных, файлам и т. п. Поэтому, определяя техническую ПБ, нужно установить, насколько можно доверять людям и информационным ресурсам, поскольку возможны атаки с подменой ("маскарадом") ресурсов (spoofing).

Кроме этого, ПБ могут создаваться для отдельных пользователей или группы пользователей – для отдельного департамента, роли/должности, внутри организации или за ее пределами (для партнеров, клиентов, аудиторов и т. п.). Итак, будем рассматривать ПБ организации как документацию, определяющую высокоуровневые цели, содержание и основные направления и устанавливающую правила, процедуры, практические приемы и руководящие принципы ОИБ активов организации, которыми она руководствуется в своей деятельности.

В соответствии с целями безопасности и стратегией, принятой организацией для достижения этих целей, определяется надлежащий уровень детализации ПБ ИТКС организации. Политика безопасности ИТКС должна распространяться:

- на предмет и задачи безопасности;
- цели безопасности с учетом правовых и регулирующих обязательств, а также направления деятельности организации;
- ссылки на стандарты, лежащие в основе данной политики;
- требования безопасности к обеспечению конфиденциальности, целостности, доступности, безотказности, подотчетности и аутентичности информации и средств ее обработки;
- администрирование ИБ, охватывающее организационную и индивидуальную ответственность и полномочия;
- подход к управлению риском, принятый в организации;
- метод определения приоритетов реализации защитных мер;

В соответствии с целями безопасности и стратегией, принятой организацией для достижения этих целей, определяется надлежащий уровень детализации ПБ ИТКС организации. Политика безопасности ИТКС должна распространяться:

- уровень безопасности и остаточный риск, определяемый руководством организации;
- общие правила контроля доступа (логический, а также контроль физического доступа в здания, помещения, к системам и информации);
- подходы к осведомленности о безопасности и повышение квалификации в области безопасности в рамках организации;
- процедуры проверки и поддержания безопасности;
- общие вопросы о защите персонала;
- способы, которыми ПБ будет доведена до сведения всех заинтересованных лиц;
- условия анализа или аудита политики безопасности;
- метод контроля изменений в политике безопасности.

Первый учебный вопрос.

Организации должны оценить свои требования, окружающую среду и уровень развития и определить наиболее отвечающую им специфическую проблему безопасности, включающую в себя:

- требования безопасности (например, требования конфиденциальности, целостности, доступности, безотказности, аутентичности и достоверности);
- организационную инфраструктуру и распределение обязанностей;
- интеграцию безопасности при совершенствовании системы и закупках;
- определение методов и уровней классификации информации;
- стратегию управления рисками;
- вопросы, связанные с персоналом (особое внимание должно быть уделено сотрудникам, занимающим ответственные должности);
- осведомленность и обучение персонала;
- правовые и регулирующие обязательства;
- менеджмент, осуществляемый независимым экспертом;
- управление инцидентами информационной безопасности.

Первый учебный вопрос.

Как отмечено выше, результаты исследований по оценке риска, проверок соответствия безопасности и инцидентов безопасности могут оказывать влияние на ПБ организации путем пересмотра ранее определенной стратегии или ПБ.

Перечисленные в ПБ мероприятия, касающиеся проблем обеспечения ИБ, могут основываться на целях и стратегии организации; результатах проведенного ранее анализа риска систем безопасности и принципов управления; результатах проведения дополнительных мероприятий, таких как проверка действенности состояния реализованных защитных мер; результатах мониторинга и изучения процесса повседневного использования систем безопасности, а также на содержании отчетов об экстренных ситуациях, связанных с вопросами в сфере обеспечения безопасности.

Первый учебный вопрос.

Необходимо рассматривать любые случаи обнаружения серьезных угроз или уязвимостей в системе безопасности, а ПБ должна содержать описание общих методов подхода организации к решению указанных проблем при обеспечении безопасности. Более подробно методы и действия по обеспечению безопасности систем информационных технологий описываются в ПБ различных ИТКС. В разработке ПБ должны принимать участие руководство организации и персонал:

- служб аудита;
- финансовых служб;
- подразделений, обслуживающих ИТКС и пользователей;
- служб безопасности.

Первый учебный вопрос.

В соответствии с целями безопасности и стратегией, принятой организацией для их достижения, выбирается соответствующий уровень детализации ПБ. Описание этой политики должно включать в себя по меньшей мере следующую информацию:

- сведения о ее целях и области применения;
- цели системы обеспечения безопасности и их соотношение с правовыми и нормативными обязательствами и целями организации;
- требования, предъявляемые к системе обеспечения безопасности с точки зрения обеспечения конфиденциальности, целостности, доступности, достоверности и надежности информации;
- сведения об общем уровне безопасности и остаточном риске, необходимые для осуществления управления;
- сведения об управлении безопасностью, включающие в себя данные об ответственности и полномочиях как организации, так и от дельных лиц;
- вариант подхода к управлению риском, принятый организацией;

- пути и способы определения приоритетов при реализации защитных мер;
- данные о наличии общих правил контроля доступа (контроль доступа при физическом доступе лиц в здания, рабочие помещения, а также к системам и информации);
- сведения о доведении до персонала мер безопасности и обучении лиц, осуществляемом организацией;
- данные об общих процедурах контроля и поддержания без опасности;
- перечень общих проблем обеспечения безопасности, касающихся обслуживающего персонала;
- средства и способы доведения сути политики безопасности информационных технологий до всех заинтересованных лиц;
- обстоятельства, при которых может быть пересмотрена ПБ;
- методы контроля изменений, вносимых в ПБ организации.

Первый учебный вопрос.

При разработке ПБ с более высокой степенью детализации должны быть дополнительно рассмотрены следующие вопросы:

- использование стандартов;
- процедуры внедрения защитных мер;
- модели и процедуры обеспечения безопасности, распространяющиеся на все подразделения организации;
- проверка действенности систем обеспечения безопасности;
- мониторинг использования средств безопасности;
- обработка инцидентов, связанных с нарушением ИБ;
- мониторинг функционирования ИТКС;
- обстоятельства, при которых требуется приглашение сторон них экспертов по проблемам в сфере ИБ.

Результаты анализа риска и принципов управления, проверки действующей системы безопасности и инцидентов, связанных с нарушением безопасности, могут отразиться на содержании ПБ ИТ, что, в свою очередь, может привести к пересмотру или доработке ранее сформулированной ПБ.

Для обеспечения поддержки проведения мероприятий, связанных с вопросами безопасности, необходимо одобрение ПБ высшим руководством организации. На основе содержания ПБ требуется сформулировать директиву, обязательную для всех руководящих работников и сотрудников.

При этом может потребоваться получение подписи каждого сотрудника на документе, содержащем положения о его ответственности за поддержание безопасности в пределах организации. Кроме того, должна быть разработана и реализована программа по обеспечению знания и понимания мер безопасности и проведено обучение использованию этих мер.

Первый учебный вопрос.

Должно быть назначено лицо, ответственное за реализацию политики безопасности информационных технологий и обеспечение соответствия политики требованиям и реальному состоянию дел в организации. Обычно таким ответственным лицом в организации является сотрудник службы безопасности информационных технологий, помимо своих должностных обязанностей отвечающий и за проведение дополнительных мероприятий, которые должны включать в себя контрольный анализ действующих защитных мер, обработку инцидентов, связанных с нарушением системы безопасности и обнаружением уязвимостей в системе, а также с внесением изменений в содержание политики безопасности, если в результате проведенных мероприятий возникнет такая необходимость.

Второй учебный вопрос.

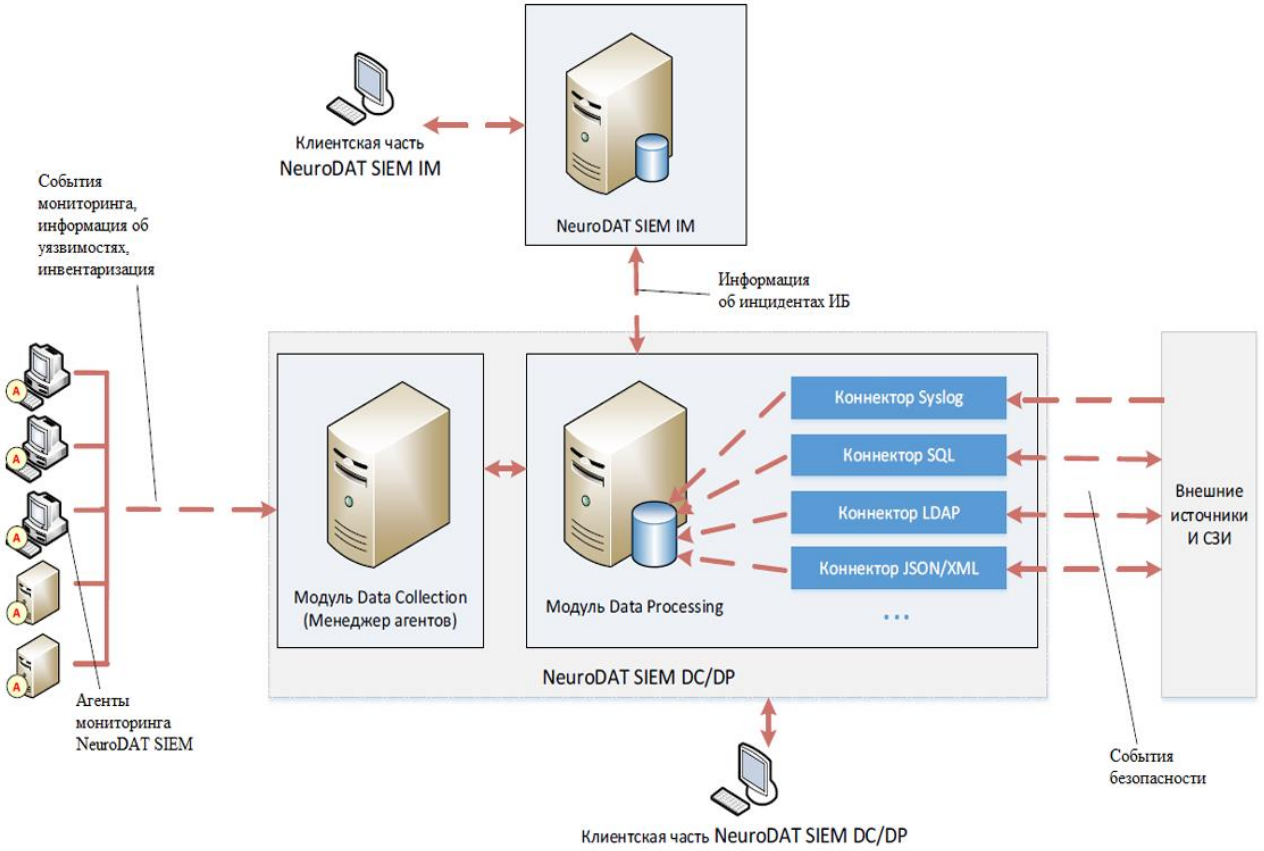
Назначение, состав и возможности *NeuroDAT SIEM*

Второй учебный вопрос.

Основной задачей центра NeuroDAT SIEM является обеспечение организации процесса мониторинга информационной безопасности. Источниками событий безопасности для NeuroDAT SIEM могут выступать различные средства защиты информации, бизнес-приложения, сетевые устройства и др. Также для получения информации от пользовательских автоматизированных рабочих мест (АРМ) и сер веров может устанавливаться агент мониторинга NeuroDAT. В связи с этим возникает необходимость разработки учебно-тренировочного комплекса по применению NeuroDAT SIEM для подготовки сотрудников Центра мониторинга информационной безопасности.

Второй учебный вопрос.

Архитектура NeuroDAT SIEM



Второй учебный вопрос.

Для применения NeuroDAT SIEM рекомендуется использовать средство виртуализации, которое позволит увеличить эффективность и гибкость использования данной системы без необходимости покупки дополнительного оборудования. При выборе средства виртуализации для применения NeuroDAT SIEM важно учитывать следующие критерии:

1) совместимость – выбранная система виртуализации должна быть совместима с операционной системой, на которой будет работать NeuroDAT SIEM;
2) производительность – виртуализация может негативно влиять на производительность системы. Поэтому важно выбрать средство виртуализации, которое обеспечивает высокую производительность и минимальные задержки при работе с NeuroDAT SIEM;
3) масштабируемость – средство виртуализации должно позволять масштабировать систему NeuroDAT SIEM в зависимости от потребностей. Это позволит гибко настраивать систему под текущие требования, а также расширять ее в будущем;
4) удобство управления – выбранное средство виртуализации должно обеспечивать удобный и простой интерфейс управления, который позволит легко настраивать и контролировать работу системы.

Второй учебный вопрос.

Если информация, обрабатываемая ПО системы мониторинга ИБ NeuroDAT SIEM IM, признана пользователем общедоступной, то состав среды функционирования ПО системы мониторинга ИБ NeuroDAT SIEM IM должен быть следующий:

- операционная система специального назначения Astra Linux Special Edition РУСБ.10015-01 (версия 1.6) с установленным кумулятивным обновлением для нейтрализации угроз эксплуатации уязвимостей (Бюллетень № 20200327SE16 – Update-5);
- JRE 1.8 (ревизия 241) – среда для обеспечения функционирования веб-сервера apache tomcat 8.5.53, разработанного на языке программирования Java.

Веб-сервер apache tomcat 8.5.53 – приложение, запускаемое в качестве службы операционной системы, в составе которого функционируют следующие модули ПО СМИБ NeuroDAT SIEM IM:

1) веб-модуль для обработки http-запросов пользователей приложения и выдачи пользователям различных экранных форм для отображения и ввода данных;
2) логический модуль для выполнения различных расчетов с данными и их преобразования;
3) модуль управления данными, обеспечивающий взаимодействие с базой данных PostgreSQL 9.6.10 для чтения, записи данных, выполнения поисковых запросов различного вида.

PostgreSQL 9.6.10 – СУБД, входящая в состав сертифицирован ной ОС специального назначения Astra Linux Special Edition РУСБ.10015-01 (версия 1.6) с установленным кумулятивным обновлением для нейтрализации угроз эксплуатации уязвимостей (Бюллетень № 20200327SE16 – Update-5), обеспечивающая хранение данных ПО СМИБ NeuroDAT SIEM IM. Взаимодействует с модулем управления данными приложения, функционирующего в контексте веб-сервера apache tomcat 8.5.53.

Веб-браузер – клиентское приложение, установленное на персо нальном компьютере пользователя ПО СМИБ NeuroDAT SIEM IM, через которое выполняется доступ к функциям ПО СМИБ NeuroDAT SIEM IM. Рекомендуется использовать один из следующих браузеров:

- Mozilla Firefox (версия 54 и выше);
- Chrome (версия 58 и выше);
- Яндекс.Браузер (версия 18.11.1).

Если информация, обрабатываемая ПО СМИБ NeuroDAT SIEM IM, признана пользователем информацией ограниченного доступа, то в среде ее функционирования должны применяться механизмы за щиты информации ОС, СУБД и (или) иных средств защиты информации, прошедшие оценку соответствия требованиям по без опасности в формах, установленных законодательством.

Состав среды функционирования ПО СМИБ NeuroDAT SIEM IM должен быть следующий:

– операционная система специального назначения Astra Linux Special Edition РУСБ.10015-01 (версия 1.6) с установленным кумулятивным обновлением для нейтрализации угроз эксплуатации уязвимостей (Бюллетень № 20200327SE16 – Update-5);

– JRE 1.8 (ревизия 241) – среда для обеспечения функциониро вания веб-сервера apache tomcat 8.5.53, разработанного на языке программирования Java.

Второй учебный вопрос.

Веб-сервер apache tomcat 8.5.53 – приложение, запускаемое в качестве службы операционной системы, в составе которого функционируют следующие модули ПО СМИБ NeuroDAT SIEM IM:

- веб-модуль для обработки http-запросов пользователей приложения и выдачи пользователям различных экранных форм для отображения и ввода данных;
- логический модуль для выполнения различных расчетов с данными и их преобразования;
- модуль управления данными, обеспечивающий взаимодействие с базой данных Postgres Pro Standard v.9.6.3.1 для чтения, записи данных, выполнения поисковых запросов различного вида.

Сертифицированная СУБД Postgres Pro Standard v.9.6.3.1 – СУБД, обеспечивающая хранение данных ПО СМИБ NeuroDAT SIEM IM. Взаимодействует с модулем управления данными приложения, функционирующего в контексте веб-сервера apache tomcat 8.5.53.

Веб-браузер – клиентское приложение, установленное на персональном компьютере пользователя ПО СМИБ NeuroDAT SIEM IM, через которое выполняется доступ к функциям ПО СМИБ NeuroDAT SIEM IM.

Рекомендуется использовать один из следующих браузеров:

- Mozilla Firefox (версия 54 и выше);
- Chrome (версия 58 и выше);
- Яндекс.Браузер (версия 18.11.1).

Второй учебный вопрос.

Алгоритм функционирования учебно-тренировочного комплекса на базе среды виртуализации для применения NeuroDAT SIEM может быть следующим:

1. Установка среды виртуализации, такой как VMWare ESXi или Microsoft Hyper-V, на физический сервер.
2. Создание виртуальной машины в среде виртуализации для установки NeuroDAT SIEM.
3. Установка NeuroDAT SIEM на виртуальную машину.
4. Настройка параметров NeuroDAT SIEM, таких как настройки сети и аутентификации.
5. Настройка параметров среды виртуализации, таких как выделение ресурсов, мониторинг и резервное копирование.
6. Создание виртуальных машин для учебных целей, например для имитации атаки и мониторинга с помощью NeuroDAT SIEM.
7. Настройка сетевых параметров виртуальных машин для их подключения к NeuroDAT SIEM.
8. Запуск учебных сценариев на виртуальных машинах и мониторинг их работы с помощью NeuroDAT SIEM.
9. Анализ результатов мониторинга и корректировка настроек NeuroDAT SIEM и среды виртуализации для улучшения производительности и защиты от атак.
10. Проведение регулярных тестов и обновлений системы для поддержания ее работоспособности и безопасности.

Второй учебный вопрос.

В соответствии с заданием на дипломное проектирование учебно-тренировочный комплекс должен наглядно отображать обнаружение и регистрацию инцидентов информационной безопасности с помощью NeuroDAT SIEM.

Компоненты NeuroDAT SIEM DC/DP и NeuroDAT SIEM DA имеют трехуровневую архитектуру:

- база данных;
- сервер приложений;
- клиентские приложения.

База данных содержит данные, используемые NeuroDAT SIEM DC/DP и NeuroDAT SIEM DA в процессе функционирования. В качестве системы управления БД применяется PostgreSQL.

Сервер приложений используется для взаимодействия клиентских частей с БД, между собой, а также для выполнения различных служебных и фоновых задач. В контекстах ЦСОД и ЦАД сервер приложений имеет название "служба координации запросов" (координатор).

Клиентские приложения выполняют функции интерфейса пользователя, а также интерфейсов взаимодействия NeuroDAT SIEM со сторонними системами.

В процессе функционирования клиентские приложения соединяются со службой координации запросов для обмена с ней данными. К клиентским приложениям относятся АРМ оператора ЦАД (консоль управления ЦАД), АРМ оператора ЦСОД (консоль управления ЦСОД), приложения с оконным графическим интерфейсом пользователя, имеющие функцию автоматического обновления и не требующие ручной переустановки (обновленная версия загружается с сервера)

Второй учебный вопрос.

Специализированные службы (применимы только для ЦСОД) выполняют функции интерфейсов взаимодействия между отдельными компонентами ЦСОД, а также со сторонними системами. К специализированным службам относятся:

- менеджер агентов, осуществляющий все виды взаимодействия (управление, прием данных) с агентами NeuroDAT SIEM, установленными на контролируемых системой ПЭВМ и серверах под управлением MS Windows;
- коннекторы к сторонним системам – поставщикам событий.

В качестве поставщиков событий рассматриваются:

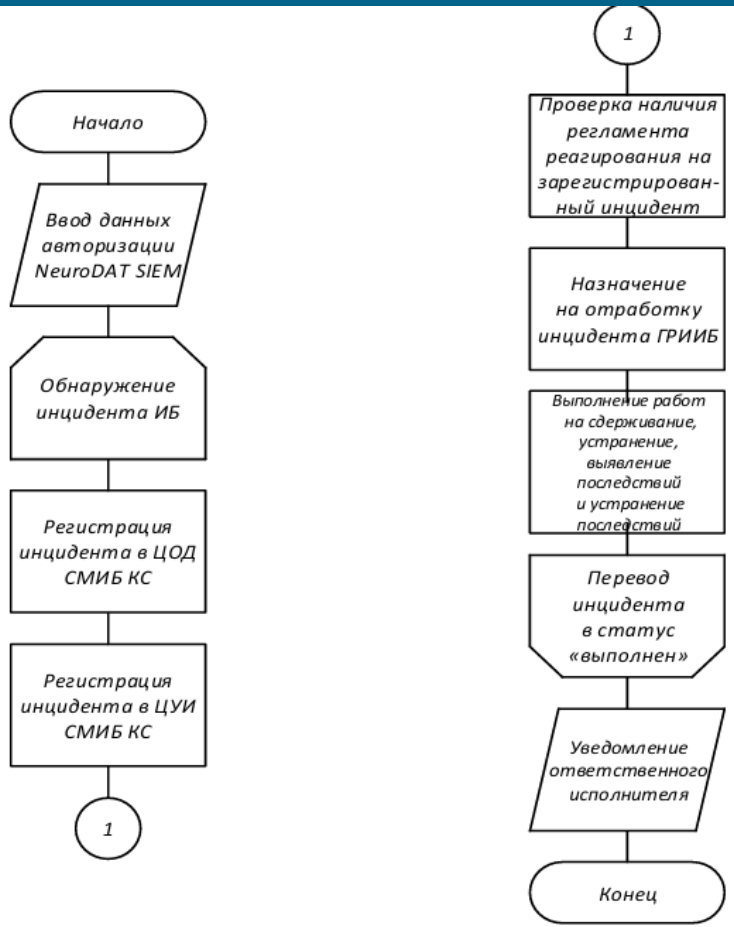
- системы обнаружения атак (IPS, IDS);
- антивирусные системы;
- DLP-системы;
- серверы LDAP, DNS, PROXY, DHSP и др.;
- СУБД;
- коммутационное оборудование;
- прикладные автоматизированные системы;
- межсетевые экраны;
- другое оборудование и программное обеспечение, формирующие события безопасности.

Второй учебный вопрос.

После прохождения процедуры идентификации и аутентификации пользователю будет доступен интерфейс для работы с системой в соответствии с его правами доступа (определяемыми соответствующей "ролью" пользователя в системе).

Исходя из вышеуказанного, можно разработать методику реагирования на инциденты информационной безопасности в NeuroDAT SIEM IM.

Второй учебный вопрос.



Методика реагирования на инциденты информационной безопасности в NeuroDAT SIEM IM

Второй учебный вопрос.

Группа реагирования на инциденты (ГРИИБ) формируется из числа сотрудников, участвующих в процессе реагирования на инцидент в соответствии с регламентами выявления, регистрации и реагирования на инциденты.

Состав ГРИИБ:

- руководитель ГРИИБ;
- заместитель руководителя ГРИИБ;
- ответственные исполнители.

Второй учебный вопрос.

Функции руководителя ГРИИБ и его заместителя:

- назначение ГРИИБ на отработку инцидента;
- назначение ответственного исполнителя инцидента из состава ГРИИБ;
- назначение ответственных исполнителей заданий по реагированию на инцидент из состава ГРИИБ;
- переназначение ответственного исполнителя инцидента из со става ГРИИБ;
- переназначение ответственных исполнителей заданий по реагированию на инцидент из состава ГРИИБ;
- подтверждение закрытия инцидента;
- возврат в работу инцидента;
- назначение руководителя ГРИИБ или заместителя руководи теля ГРИИБ ответственным исполнителем инцидента;
- назначение руководителя ГРИИБ или заместителя руководи теля ГРИИБ ответственным исполнителем заданий по реагированию на инцидент.

Второй учебный вопрос.

Руководитель ГРИИБ или его заместитель может назначить ответственного исполнителя инцидента и завершить работы по инциденту.

Режим работы ГРИИБ в текущей версии СМИБ NeuroDAT SIEM IM следующий: пять дней в неделю, с понедельника по пятницу, 8 ч в день, с учетом производственного календаря.
Начало и окончание рабочего дня определяются параметрами: "Режим работы ГРИИБ (от)", "Режим работы ГРИИБ (до)". Обед – 1 ч спустя 4 ч с начала рабочего дня.
Режим работы ГРИИБ влияет на автоматический расчет значения крайнего срока инцидента с учетом объема времени, определенного в регламентах реагирования на инциденты.
Представ ленные параметры определения режима работы ГРИИБ в новой версии СМИБ NeuroDAT SIEM IM будут настраиваться пользователем.

Второй учебный вопрос.

Работа с функциями АРМ оператора ЦСОД и ЦАД производится с помощью унифицированного графического интерфейса пользователя, при проектировании и разработке которого использовались следующие принципы:

1. Неблокируемый интерфейс. При работе с какой-либо функцией приложения всегда можно временно переключиться на одну или несколько других функций. При этом работа с предыдущей функцией не прекращается и может быть продолжена в любой момент. Это достигается применением интерфейса, основанного на так называемых вкладках. Подход с применением вкладок позаимствован у современных интернет-обозревателей (браузеров) как наиболее удобный и привычный большинству пользователей.

2. Асинхронный характер выполнения длительных операций. Операции, которые потенциально могут выполняться длительное время, такие как загрузка больших массивов данных либо выполнение сложных аналитических запросов, выполняются в фоновом режиме. Это позволяет продолжить работу с другими функциями приложения без блокировки работы и ожидания.

3. Унифицированный подход при работе с экранными формами. Работа со всеми функциями приложения основана на использовании одной или нескольких экранных форм, являющихся довольно разнообразными, что связано с широкой функциональной насыщенностью приложения. Однако для удобства пользователя все экранные формы имеют общую структуру и состоят из набора однотипных блоков (панелей).

Второй учебный вопрос.

АРМ оператора ЦСОД содержит множество функций. Вызов любой функции осуществляется при помощи главного меню приложения, которое состоит из следующих пунктов:

1) общие – управляющие функции общего характера;
2) данные мониторинга – функции по просмотру и анализу данных, поступающих от различных систем мониторинга ИБ;
3) агенты – функции по управлению агентами мониторинга;
4) узлы – функции по просмотру и управлению перечнем узлов, зарегистрированных в NeuroDAT SIEM;
5) инциденты – функции по просмотру и управлению перечнем инцидентов ИБ, зарегистрированных в NeuroDAT SIEM;
6) карты – функции по просмотру в статическом и динамическом режимах информации о внешних (из сети Интернет) компьютерных атаках на сеть организации (при условии наличия в сети организации СЗИ типа IDS);
7) файлы – функции по работе с файлами, которые хранятся внутри БД NeuroDAT SIEM и могут быть использованы в качестве приложений при описании инцидентов ИБ;
8) контроль – функции по контролю работоспособности источников событий;
9) администрирование – функции администрирования Neurodat SIEM.

Особенности функционирования Центра мониторинга информационной безопасности NeuroDAT SIEM

Программное обеспечение "Система мониторинга информаци онной безопасности NeuroDAT SIEM Incident Management" (далее СМИБ NeuroDAT SIEM IM) решает задачи управления процессом устранения зарегистрированных инцидентов путем автоматизации регламентов реагирования на такие инциденты. ПО СМИБ NeuroDAT SIEM IM выполняет следующие функции:

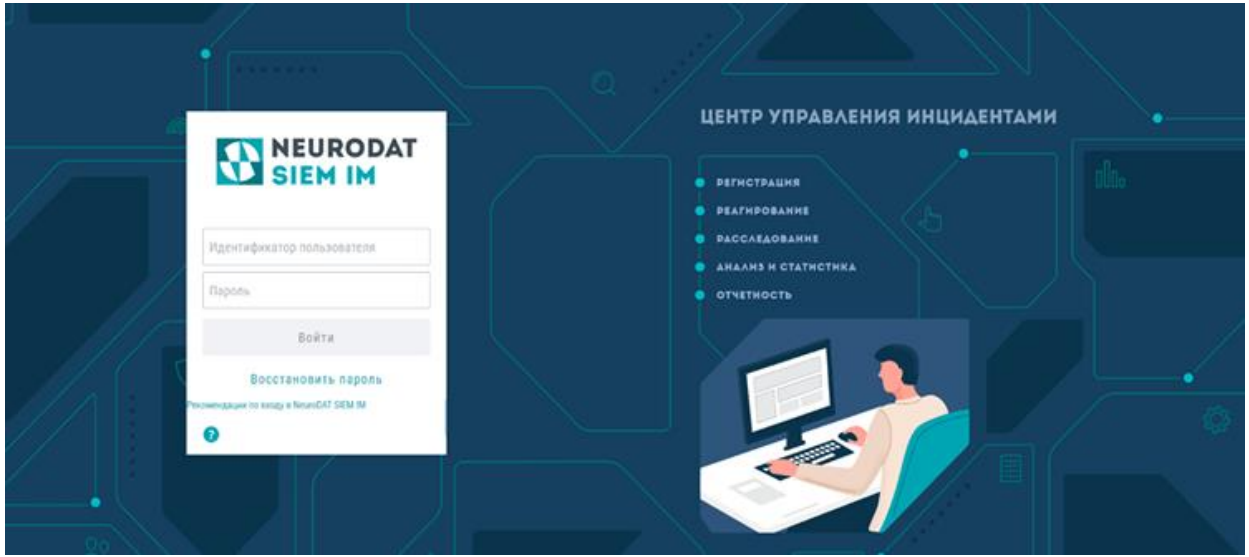
- регистрация новых пользователей с последующим назначением функциональных возможностей в соответствии с назначенной пользователю ролью;
- формирование организационной структуры, предназначенной для выполнения заданий по реагированию на инциденты – группы реагирования на инциденты;
- настройка требований к паролю пользователя;
- контроль правил генерации и смены паролей пользователей;

- настройка значений индикаторов нагрузки на приложение, автоматический контроль индикаторов и автоматическая перезагрузка приложения при длительном превышении значений индикаторов;
- автоматическое уведомление администратора о превышении значений индикаторов;
- автоматическое уведомление администратора о пользователях, заблокированных в результате нарушения идентификации и аутентификации;
- создание автоматизированных регламентов реагирования на инциденты, содержащих редактируемые формализованные задания для ответственных за устранение инцидентов;
- регистрация данных по выявленным инцидентам;
- автоматическое уведомление о регистрации нового инцидента (электронная почта, мгновенное сообщение в интерфейсе ПО СМИБ NeuroDAT SIEM IM) руководителя группы реагирования на инциденты;

- автоматическое назначение ответственных исполнителей за отработку инцидента;
- назначение руководителем группы реагирования на инциденты ответственного исполнителя инцидента;
- автоматическое уведомление (электронная почта, мгновенное сообщение в интерфейсе ПО СМИБ NeuroDAT SIEM IM) назначенного ответственного исполнителя инцидента;
- автоматизированное формирование ответственным исполнителем инцидента заданий по реагированию на инцидент в соответствии с регламентом реагирования на инцидент;
- назначение ответственным исполнителем инцидента ответ ственных исполнителей заданий по реагированию на инцидент; автоматическое уведомление (электронная почта, мгновенное сообщение в интерфейсе ПО СМИБ NeuroDAT SIEM IM) назначенного ответственного исполнителя задания по реагированию на инцидент;

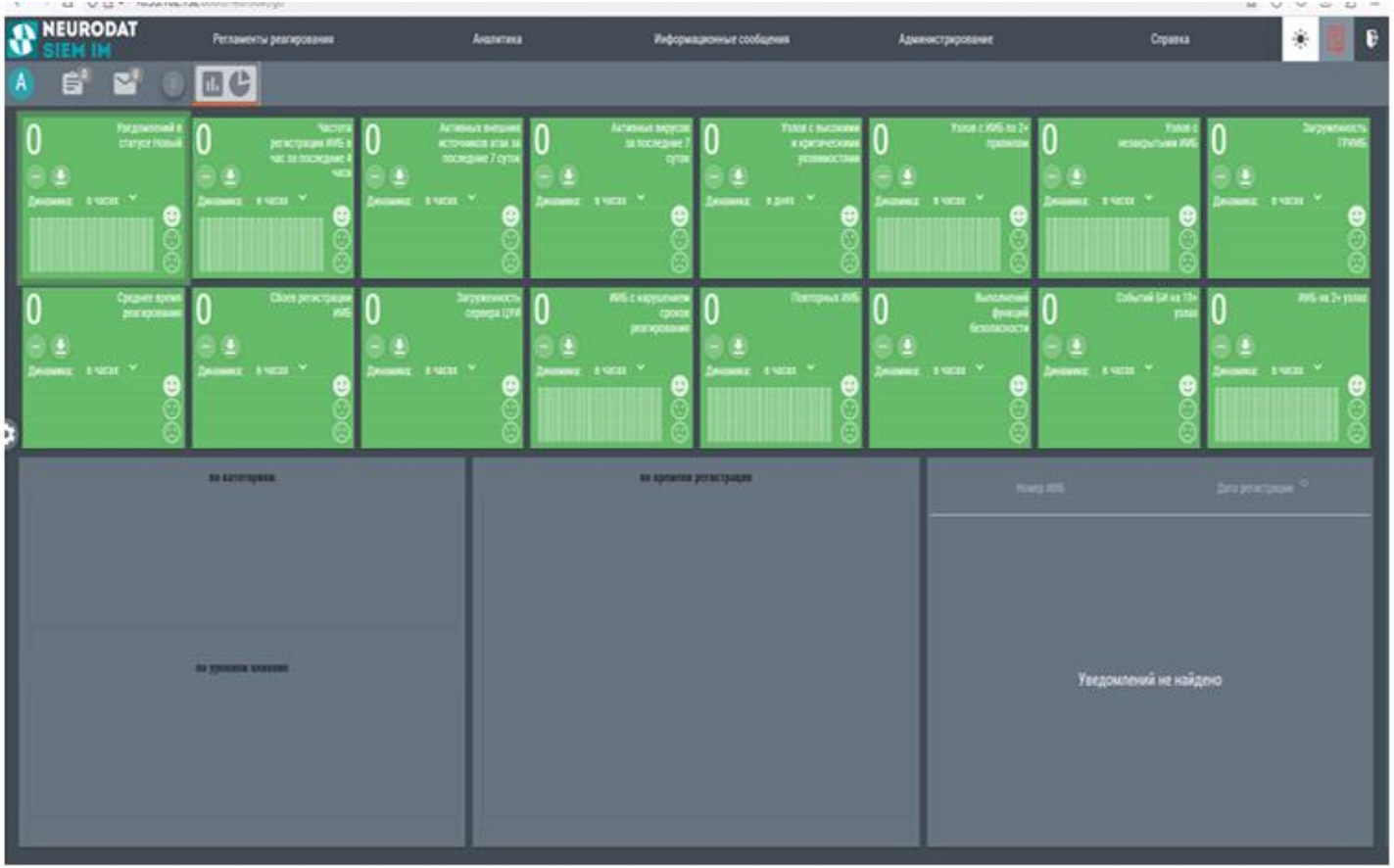
- контроль сроков реагирования и действий, выполненных ответственными исполнителями в рамках заданий по реагированию на инциденты;
- автоматическое уведомление (электронная почта, мгновенное сообщение в интерфейсе ПО СМИБ NeuroDAT SIEM IM) ответственного исполнителя инцидента о факте нарушения сроков реагирования на инцидент;
- графическое представление количественных показателей по зарегистрированным инцидентам с детализацией по объекту контроля, времени регистрации, категории и статусу инцидента, уровню его влияния;
- ведение сводной и сравнительной статистической отчетности с возможностью выгрузки в файл формата .xls, .xlsx информации о зарегистрированных инцидентах с детализацией по объекту контроля, времени регистрации, категории и статусу инцидента, уровню его влияния на общее состояние информационной безопасности системы.

ПО СМИБ NeuroDAT SIEM IM функционирует круглосуточно, кроме периодов проведения администратором ПО СМИБ NeuroDAT SIEM IM технологических работ, требующих остановку ПО. Периодичность, длительность и время проведения технологических работ указаны в руководстве администратора ПО СМИБ NeuroDAT SIEM IM



Пользовательская часть ПО СМИБ NeuroDAT SIEM IM является веб-приложением и не требует дополнительной установки на рабочих местах зарегистрированных пользователей. Для работы с ПО СМИБ NeuroDAT SIEM IM пользователям рекомендуется использовать один из следующих браузеров: Яндекс.Браузер (версия 18.11.1); Mozilla Firefox (версия 54 и выше); Chrome (версия 58 и выше).

В СМИБ NeuroDAT SIEM IM реализованы механизмы обработки отказов аутентификации при вводе пользователем неправильного идентификатора пользователя или пароля. В СМИБ NeuroDAT SIEM IM в окне идентификации и аутентификации пользователя после заполнения полей "Идентификатор пользователя", "Пароль" и нажатия на кнопку "Продолжить" выполняется проверка заполненных полей. Если поле "Идентификатор пользователя" содержит неправильное значение, появляется сообщение "Введен неправильный идентификатор пользователя или пароль".



Интерфейс веб-приложения центра мониторинга NeuroDAT SIEM IM

Основной формой мониторинга за процессом управления инцидентами является "Состояние ИБ". Форма "Состояние ИБ" автоматически обновляется каждые 3 мин. Но возможны ситуации, когда пользователю не потребуется работать с формой длительное время (открывать объекты, содержащиеся на форме).

С целью исключения постоянного завершения пользовательской сессии в результате неактивности более определенного количества минут для формы "Состояние ИБ" устанавливается отдельное значение срока завершения пользовательской сессии. Если открыта форма "Состояние ИБ", сессия продолжается.

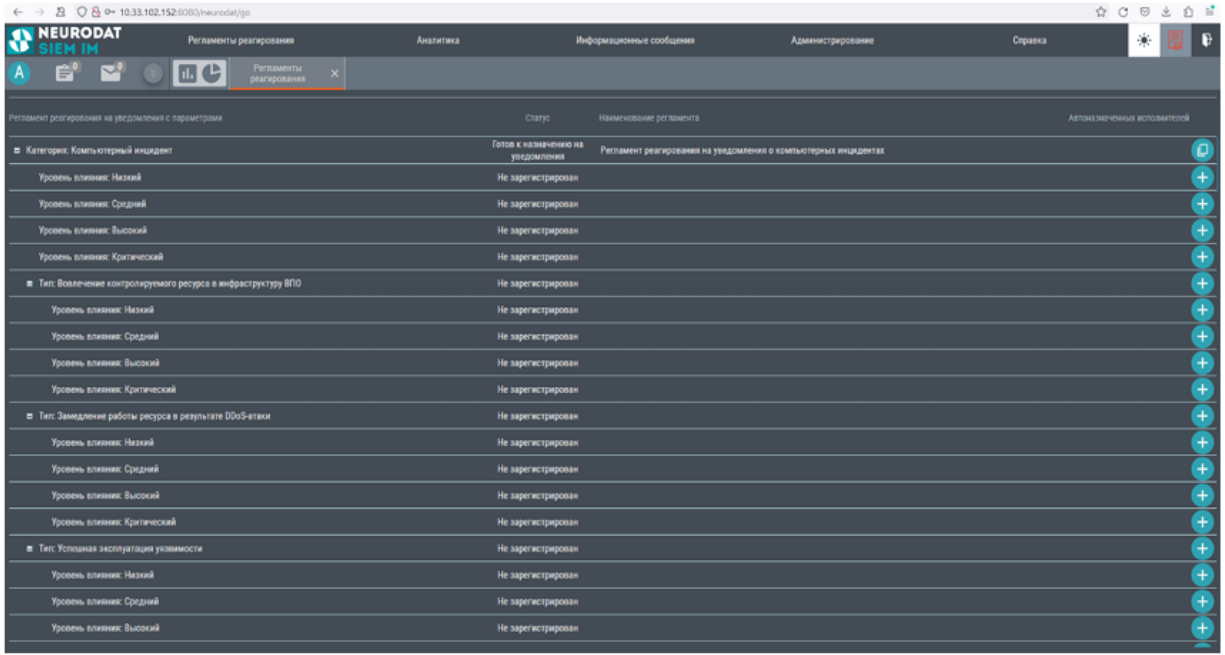
Если форма "Состояние ИБ" непрерывно активна более определенного количества часов, то выдается сообщение "Отсутствие активности пользователя более N часов".

Функции регистрации и удаления объекта "Подразделение" доступны зарегистрированным пользователям с ролью "Администратор". Пункт меню "Подразделение" содержит список зарегистрированных пользователей. Вложенность пунктов, входящих в подразделение, может быть многоуровневой. Порядок регистрации объекта "Подразделение" Открыть браузер.

В адресной строке ввести: http://[ip-адрес сер вера приложения СМИБ NeuroDAT SIEM IM]:8080/neurodat/go.

В форме идентификации и аутентификации пользователя заполнить поля "Идентификатор пользователя", "Пароль" (admin/********). Перейти в пункт меню "Администрирование – Структура организации", в результате откроется форма "Структура организации". В форме "Структура организации" напротив наименования за регистрированной зоны ответственности нажать на кнопку "Новое подразделение", в результате откроется форма "Подразделение".

В форме "Подразделение" заполнить обязательные поля "Наименование", "Краткое наименование" и нажать кнопку "Сохранить" (рис.). Зарегистрированное подразделение появится в соответствующем списке формы "Структура организации".



Функции регистрации и копирования объекта "Регламент реагирования на инциденты" доступны зарегистрированным пользователям с ролью "Администратор".

Регламент реагирования на инциденты содержит упорядоченный набор рекомендуемых заданий, направленных на устранение инцидента и его последствий. Регламенты реагирования на инциденты автоматически назначаются на новые зарегистрированные инциденты категории, соответствующей категории регламента.

Для одной категории инцидентов может быть зарегистрирован только один регламент. В рамках категории возможно создавать регламенты на правило регистрации инцидентов. Также пользователям с ролью "Администратор" при работе с регламентом доступны функции копирования и удаления регламента.

Регистрация объекта "Регламент реагирования на инциденты" выполняется в следующем порядке:

- Открыть браузер. В адресной строке ввести: http://[ip-адрес сер вера приложения СМИБ NeuroDAT SIEM IM]:8080/neurodat/go.

В форме идентификации и аутентификации пользователя заполнить поля "Идентификатор пользователя", "Пароль" (указать значения ранее созданного пользователя с ролью "Администратор").

Перейти в пункт меню "База знаний – Регламенты", в результате откроется форма "Регламенты", содержащая список ранее зарегистрированных регламентов для всех возможных категорий инцидентов.

В форме "Регламенты" нажать на кнопку "Добавить регламент", в результате появится форма "Новый регламент". В форме "Новый регламент" заполнить следующие поля:

- "Наименование регламента" (текстовое поле);
- "Категория" (поле содержит список зарегистрированных в СМИБ NeuroDAT SIEM IM категорий инцидентов, необходимо вы брать одну из категорий). Регламент выбранной категории будет автоматически назначаться на регистрируемые инциденты аналогичной категории. На одну категорию нельзя зарегистрировать более одного регламента.

Третий учебный вопрос.

В форме редактирования регламента реагирования заполнить следующие поля:

- "Наименование регламента" (текстовое поле, обязательное для заполнения);
- "Категория" (поле заполняется автоматически значением, выбранным в форме "Новый регламент");
- "Правила регистрации инцидентов" (поле содержит список зарегистрированных правил регистрации инцидентов в СМИБ NeuroDAT SIEM IM, пользователю доступна возможность выбора одного и более правил). Данная настройка позволяет создавать регламенты на каждое правило или группу правил регистрации инцидентов. Если правила не выбраны, то регламент будет автоматически назначаться на инциденты категории, указанной в поле "Категория". На одно правило нельзя зарегистрировать более одного регламента;
- "Назначение" (текстовое поле, необязательное для заполнения);
- "Файл электронной версии" (в данном поле пользователю доступна возможность прикрепить файл регламента в формате .doc/.docx, прикрепленный файл будет доступен для сохранения на жесткий диск пользователями, зарегистрированными СМИБ NeuroDAT SIEM IM);
- "Статус" (поле содержит список, содержащий два значения: "Подготовка регламента", "Готов к назначению на инциденты", пользователю доступен выбор только одного из них). Созданный регламент будет автоматически назначаться на инциденты ИБ соответствующей категории после установки в поле "Статус" значения "Готов к назначению";
- "Временные характеристики" (форма содержит поля для определения времени (в часах) выполнения сдерживания и общего срока реагирования на инцидент).

Форма "Задания по реагированию на инциденты" содержит следующие разделы:

- "Регистрация инцидента" (текстовое поле "Описание" обязательно для заполнения);
- "Сдерживание инцидента" (включает в себя два обязательных для заполнения поля: текстовое поле "Содержание задания", поле "Действие исполнителя", в котором пользователю после нажатия на кнопку доступна возможность добавить любое количество рекомендуемых действий в рамках задания по реагированию на инцидент);
- "Устранение инцидента" (содержит такие же поля, как в раз деле "Сдерживание инцидента");
- "Выявление последствий инцидента" (имеет такие же поля, как в разделе "Сдерживание инцидента");
- "Устранение последствий инцидента" (содержит такие же поля, как в разделе "Сдерживание инцидента");
- "Закрытие инцидента" (текстовое поле "Описание" обязательно для заполнения).

После заполнения обязательных параметров в поле "Статус" установить значение "Готов к назначению на инциденты" и нажать на кнопку "Сохранить", в результате запись о регламенте будет зарегистрирована в СМИБ NeuroDAT SIEM IM.

Зарегистрированный регламент будет автоматически назначаться на инциденты категории, соответствующей категории регламента. Для инцидентов низкого и среднего уровня влияния обязательным заданием по реагированию на инцидент является задание на устранение инцидента. Для инцидентов высокого и критического уровня влияния обязательными заданиями по реагированию на инцидент являются задания на сдерживание и устранение инцидента, выявление последствий инцидента и устранение его последствий. Без выполнения обязательных заданий инцидент не будет переведен в статус "Выполнен".

Оператор NeuroDAT SIEM выполняет следующую последовательность действий при реагировании на инциденты информационной безопасности:

1. Обнаружение инцидента: оператор отслеживает системные журналы, логи сетевых устройств и другие источники информации, чтобы выявить инциденты информационной безопасности, такие как попытки несанкционированного доступа к системе или вредоносных атак.
2. Классификация инцидента: оператор анализирует данные об инциденте, чтобы определить его характер и уровень угрозы. Это помогает принять правильные решения и определить, как быстро нужно реагировать на инцидент.
3. Приоритизация инцидента: оператор определяет приоритетность инцидента на основе его классификации и влияния на систему, чтобы определить, как быстро нужно реагировать и какие ресурсы нужно задействовать.

Оператор NeuroDAT SIEM выполняет следующую последовательность действий при реагировании на инциденты информационной безопасности:

4. Инцидентный ответ: оператор выполняет соответствующие действия для устранения инцидента и восстановления нормальной работы системы, такие как блокирование атакующего IP-адреса, удаление вредоносного ПО или установка патчей безопасности.
5. Анализ причин инцидента: после реагирования на инцидент оператор производит анализ причин его возникновения, чтобы предотвратить подобные инциденты в будущем. Это может включать в себя исследование уязвимостей в системе, проверку правил безопасности и обучение пользователей безопасности информации.
6. Документирование инцидента: оператор документирует все этапы реагирования на инцидент, включая классификацию, приоритизацию, ответ и анализ причин, с целью улучшения процесса реагирования на инциденты в будущем и обеспечения соответствия нормативным требованиям в области информационной безопасности.

В целом оператор NeuroDAT SIEM обеспечивает эффективную и быструю реакцию на инциденты информационной безопасности, минимизируя риски для системы и защищая данные организации. После выполнения указанных действий оператор NeuroDAT SIEM может также проводить дополнительные мероприятия для улучшения безопасности системы:

1. Оценка эффективности: оператор проводит анализ эффективности реагирования на инцидент, чтобы определить, насколько быстро и эффективно были устранены проблемы. Это позволяет выявить слабые места и улучшить процесс реагирования на инциденты в будущем.
2. Обновление правил безопасности: оператор обновляет правила безопасности системы на основе анализа причин инцидента и уязвимостей системы для предотвращения подобных инцидентов в будущем и повышения безопасности системы.
3. Обучение пользователей безопасности информации: оператор проводит обучение пользователей системы безопасности информации, чтобы уменьшить вероятность возникновения инцидентов в будущем (тренинги по безопасности, регулярные проверки безопасности и другие меры).

После выполнения указанных действий оператор NeuroDAT SIEM может также проводить дополнительные мероприятия для улучшения безопасности системы:

4. Мониторинг безопасности: оператор продолжает постоянное наблюдение системы для выявления новых угроз и инцидентов безопасности, что позволяет ему реагировать на новые угрозы и обеспечивать постоянную безопасность системы.
5. Улучшение системы безопасности: оператор внедряет улучшения системы безопасности на основе анализа инцидентов и мониторинга безопасности – установка новых инструментов безопасности, улучшение политик безопасности и другие меры. Все эти дополнительные мероприятия позволяют оператору NeuroDAT SIEM улучшать безопасность системы и предотвращать возникновение инцидентов в будущем. Регулярное проведение анализа и обновление мер безопасности являются важными компонентами поддержания безопасности информационных систем.