ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
«НОВОСИБИРСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ АВТОМАТИКИ И ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ
Кафедра Защиты информации

ОТЧЁТ ПО ПРАКТИКЕ

Учебная практика: ознакомительная практика
(наименование практики в соответствии с учебным планом)

Направление подготовки: 10.03.01 Информационная безопасность

Выполнил:

Студент Борисов А.В.
(Ф. И. О.)

Группа АБ-220

Факультет АВТ.

подпись

« » декабря 2022 г.

Проверил:

Руководитель от НГТУ Иванов А.В.
(Ф. И. О.)

Балл: _____, ECTS_____,

Оценка _____
«отлично», «хорошо», «удовлетворительно», «неуд.»

_____
подпись

«___» _____ 20__ г.

Новосибирск 2022

Содержание

Введение

Информация о безопасности и управление событиями (SIEM) автоматизирует идентификацию и разрешение инцидентов на основе встроенных бизнес-правил, чтобы помочь улучшить соответствие требованиям и предупредить персонал о критических вторжениях. ИТ-аудит, стандарты и нормативные требования в настоящее время стали важной частью повседневных обязанностей большинства предприятий. В рамках этого бремени организации тратят значительное время и энергию на тщательный анализ своей системы безопасности и журналов событий, чтобы отследить, к каким системам был получен доступ, кем, какие действия имели место и было ли это уместно. Организации все чаще обращаются к автоматизации, основанной на данных, чтобы облегчить это бремя. В результате SIEM обрела форму и обеспечила целенаправленные решения проблемы. Рынок информации о безопасности и управления событиями обусловлен чрезвычайно растущей потребностью клиентов в соблюдении требований соответствия, а также постоянной потребностью в получении информации о внешних и внутренних угрозах в режиме реального времени. Клиентам необходимо анализировать данные о событиях безопасности в режиме реального времени (для управления угрозами), а также анализировать данные журнала и составлять отчеты по ним, и в первую очередь это сделало рынок информации о безопасности и управления событиями более требовательным. Рынок остается фрагментированным, без доминирующего поставщика.

Цели:

- Изучение кафедры защиты информации.
- Изучение возможности навигации на сайте НГТУ
- Изучение значения и особенностей SIEM-систем.

Задачи:

- Изучить организацию учебного процесса на кафедре ИБ.
- Изучить организацию НИР на кафедре.
- Изучить, чем является SIEM-система.
- Изучить принципы работы системы и выяснить эффективна ли она
- Узнать, какие системы существуют на рынке в настоящее время.

Основная часть

1. Описание кафедры Защиты информации

1.1 Организация учебного процесса на кафедре

Кафедра защиты информации предоставляет обучение студентов по направлениям, представленным в таблице 1.

Таблица 1. Направления и специальности

Наименование	*Код*
Направления подготовки бакалавров	
Информационная безопасность	10.03.01
Приборостроение	12.03.01
Специальности	
Информационная безопасность автоматизированных систем	10.05.03
Направления подготовки магистров	-
Кибербезопасность информационных систем	-
Методы и средства обеспечения технической защиты информации	-
Направления подготовки аспирантов	
Управление в технических системах	-
Методы и системы защиты информации, информационная безопасность	-
Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей	-
Приборы и методы измерения (по видам измерений)	-

В рамках образовательной работы кафедра осуществляет следующую деятельность:

- Обеспечение лабораторных работ, практических занятий, семинаров, лекций, презентаций по проблемам сетевых технологий и защите информации в рамках образовательных программ.
- Разработка учебно-методических комплексов для дисциплин, по которым в лабораториях будут проводиться занятия. В связи с появлением в университете двухуровневой системы подготовки выпускников (бакалавр - магистр), кафедра проводит большую работу по разработке соответствующих учебных планов, рабочих программ и учебно-методических комплексов по всем трем уровням обучения: бакалавриат, специалитет, магистратура.
- Переподготовка кадров.

Кафедра была создана в 2005 году. Это самая молодая кафедра факультета АВТ.

На кафедре имеются специализированные учебно-научные лаборатории (технических средств защиты информации, технических средств охраны объектов, программно-аппаратных и криптографических средств защиты информации), оснащённые самым современным оборудованием.

Стратегическими партнерами кафедры являются профильные Новосибирские предприятия-лицензиаты в области обеспечения информационной безопасности, на которых студенты проходят производственно-технологическую и преддипломную практику, а также родственные кафедры Вузов г. Новосибирска, Томска, Омска, Барнаула, Красноярска.

Выпускники кафедры находят работу на предприятиях различных форм собственности. Прежде всего, лицензиатов в области информационной безопасности, в банках, органах муниципальной и государственной власти, в профильных Федеральных службах. [1]

На кафедре работают 37 преподавателей, включая 4 профессоров и 9 доцентов.

Профессорско-преподавательский состав

ФИО сотрудника	Должность	email
Аникеева Вероника Валерьевна	Ассистент	kaf_zi@corp.nstu.ru
Архипова Анастасия Борисовна	Доцент	arhipova@corp.nstu.ru
Бабичев Михаил Михайлович	Старший преподаватель	babichev@corp.nstu.ru
Белов Виктор Матвеевич	Профессор	v.m.belov@corp.nstu.ru
Быков Сергей Владимирович	Старший преподаватель	s.bykov@corp.nstu.ru
Воробьев Вячеслав Сергеевич	Ассистент	vorobev.2014@corp.nstu.ru
Гриценко Владимир Алексеевич	Профессор	v.gricenko@corp.nstu.ru
Грищенко Лев Аркадьевич	Старший преподаватель	l.grishhenko@corp.nstu.ru
Дронов Вадим Юрьевич	Старший преподаватель	dronov@corp.nstu.ru
Дронова Галина Александровна	Старший преподаватель	g.dronova@corp.nstu.ru
Ершов Иван Анатольевич	Старший преподаватель	ershov@corp.nstu.ru
Захаров Константин Владимирович	Ассистент	k.zaxarov@corp.nstu.ru
Зырянов Сергей Алексеевич	Доцент	zyryanov@corp.nstu.ru
Иванов Андрей Валерьевич	Заведующий кафедрой	andrej.ivanov@corp.nstu.ru
Киселев Антон Анатольевич	Старший преподаватель	anton.kiselev@corp.nstu.ru
Коптев Евгений Сергеевич	Доцент	koptev@corp.nstu.ru
Косов Дмитрий Леонидович	Ассистент	kaf_zi@corp.nstu.ru

Рисунок 1. Профессорско-преподавательский состав

Котов Юрий Алексеевич	Доцент	kotov@corp.nstu.ru
Кувшинов Максим Алексеевич	Ассистент	kaf_zi@corp.nstu.ru
Лаптев Дмитрий Владимирович	Доцент	d.laptev@corp.nstu.ru
Ложников Павел Сергеевич	Профессор	kaf_zi@corp.nstu.ru
Лысенко Марина Валерьевна	Ассистент	m.v.lysenko@corp.nstu.ru
Медведев Михаил Александрович	Ассистент Преподаватель-внутр.совм.	M.medvedev@corp.nstu.ru M.medvedev@corp.nstu.ru
Никрошкин Иван Владимирович	Ассистент	kaf_zi@corp.nstu.ru
Огнев Игорь Александрович	Преподаватель-внутр.совм. Ассистент	i.ognev.2016@corp.nstu.ru i.ognev.2016@corp.nstu.ru
Пермяков Руслан Анатольевич	Старший преподаватель	permyakov@corp.nstu.ru
Рева Иван Леонидович	Доцент	reva@corp.nstu.ru
Рожков Семен Андреевич	Ассистент	rozhkov.2015@corp.nstu.ru
Савиных Максим Александрович	Доцент	savinyx.2012@corp.nstu.ru
Селифанов Валентин Валерьевич	Старший преподаватель	selifanov@corp.nstu.ru
Сидорова Диана Николаевна	Старший преподаватель	d.sidorova.2013@corp.nstu.ru
Стукач Олег Владимирович	Профессор	stukach@corp.nstu.ru
Теличко Евгений Анатольевич	Старший преподаватель	telichko@corp.nstu.ru
Трубин Игорь Витальевич	Ассистент	i.trubin@corp.nstu.ru
Трушин Виктор Александрович	Доцент	trushin@corp.nstu.ru
Филюшов Владислав Юрьевич	Старший преподаватель Преподаватель-внутр.совм.	kaf_zi@corp.nstu.ru kaf_zi@corp.nstu.ru
Хиценко Владимир Евгеньевич	Доцент	xicenko@corp.nstu.ru

Рисунок 2. Профессорско-преподавательский состав

Старший преподаватель Ершов И. А.:

Рисунок 3. Ершов И.А.

Имеет 24 научные публикации, 2 научно-исследовательские работы на темы:

- Волноводный ультравысокочастотный беспроводный канал беспроводный канал связи забойной телеметрической системы
- Системные исследования обеспечения метрологической прослеживаемости методами решения задач классификации

Ершовым было написано 1 учебно-методическая работа:

Приобретение базовых навыков определения параметров высокочастотных электрических и электромагнитных сигналов.

1.2 Организация НИР на кафедре

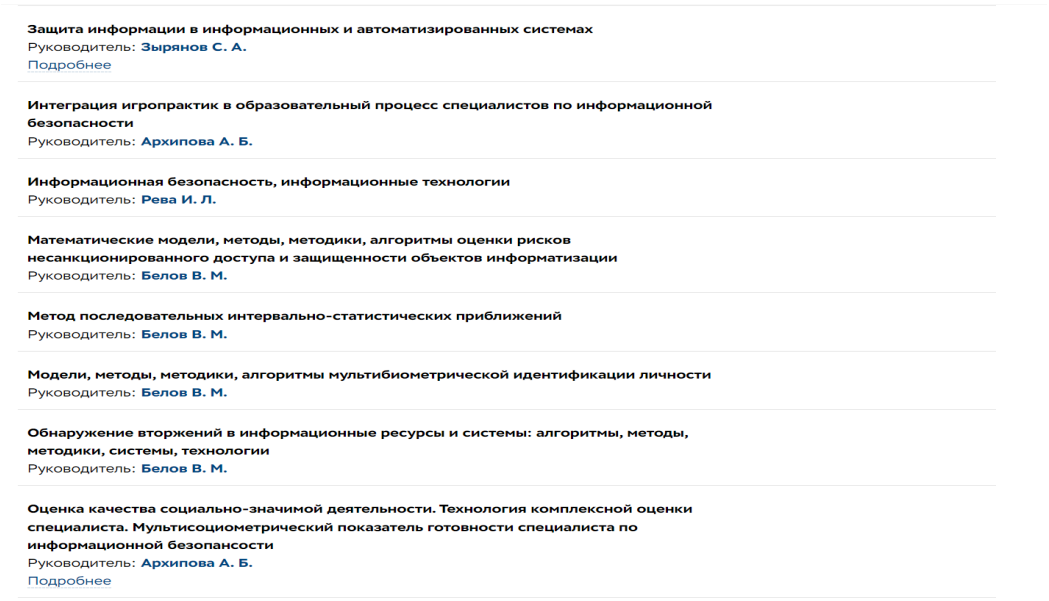
НИР студентов подразделяются на:

– учебно-исследовательскую работу студентов – работу, включаемую в учебный процесс;
– Научно-исследовательская работа студентов (НИРС), организуемая во внеучебное время, включает следующие формы:
    - участие в работе студенческих научных коллективов;
    - участие в работе проблемных научных групп на профилирующих (выпускающих) кафедрах;
    - участие в выполнении хоздоговорной тематики кафедры.

Формы и методы НИРС зависят от уровня подготовки студентов. На младших курсах преобладают такие формы НИРС как написание рефератов, выполнение расчетных работ, перевод литературы и др. На старших курсах –курсовое и дипломное проектирование, постановка и модернизация лабораторных работ, участие студентов в подготовке и проведении научных экспериментов, выполнение хоздоговорных научно-исследовательских работ.

За период с 2011 г. по 2022 г. штатными сотрудниками и совместителями было опубликовано около 500 научных работ,проверенных научной библиотекой НГТУ, 3 редакторские и составительские работы, 25 монографий, получено 25 патентов на

изобретения, 12 свидетельств на программы для ЭВМ. Кроме того, с 2013 года 4 студентов получили гранты за научные исследования.[2]



Защита информации в информационных и автоматизированных системах
Руководитель: **Зырянов С. А.**
Подробнее

Интеграция игропрактик в образовательный процесс специалистов по информационной безопасности
Руководитель: **Архипова А. Б.**

Информационная безопасность, информационные технологии
Руководитель: **Рева И. Л.**

Математические модели, методы, методики, алгоритмы оценки рисков несанкционированного доступа и защищенности объектов информатизации
Руководитель: **Белов В. М.**

Метод последовательных интервально-статистических приближений
Руководитель: **Белов В. М.**

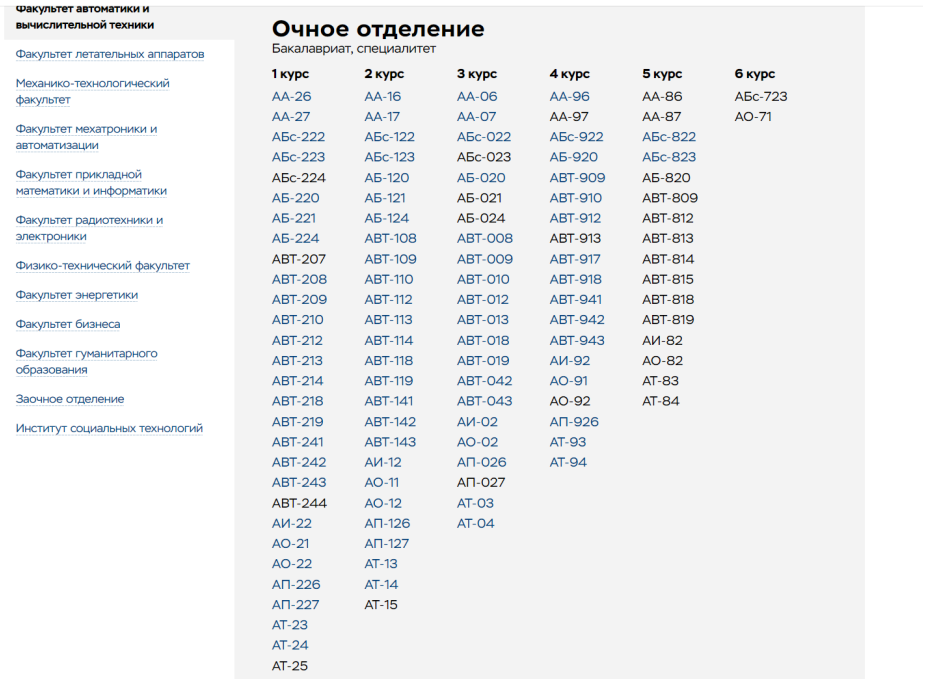
Модели, методы, методики, алгоритмы мультибиометрической идентификации личности
Руководитель: **Белов В. М.**

Обнаружение вторжений в информационные ресурсы и системы: алгоритмы, методы, методики, системы, технологии
Руководитель: **Белов В. М.**

Оценка качества социально-значимой деятельности. Технология комплексной оценки специалиста. Мультисоциометрический показатель готовности специалиста по информационной безопасности
Руководитель: **Архипова А. Б.**
Подробнее

Рисунок 2. Направления научных исследований

1.3 Возможность навигации на сайте НГТУ



Факультет автоматики и вычислительной техники

Факультет летательных аппаратов
Механико-технологический факультет
Факультет мехатроники и автоматизации
Факультет прикладной математики и информатики
Факультет радиотехники и электроники
Физико-технический факультет
Факультет энергетики
Факультет бизнеса
Факультет гуманитарного образования
Заочное отделение
Институт социальных технологий

Очное отделение
Бакалавриат, специалитет

1 курс	2 курс	3 курс	4 курс	5 курс	6 курс
АА-26	АА-16	АА-06	АА-96	АА-86	АБс-723
АА-27	АА-17	АА-07	АА-97	АА-87	АО-71
АБс-222	АБс-122	АБс-022	АБс-922	АБс-822	
АБс-223	АБс-123	АБс-023	АБ-920	АБс-823	
АБс-224	АБ-120	АБ-020	АВТ-909	АБ-820	
АБ-220	АБ-121	АБ-021	АВТ-910	АВТ-809	
АБ-221	АБ-124	АБ-024	АВТ-912	АВТ-812	
АБ-224	АВТ-108	АВТ-008	АВТ-913	АВТ-813	
АВТ-207	АВТ-109	АВТ-009	АВТ-917	АВТ-814	
АВТ-208	АВТ-110	АВТ-010	АВТ-918	АВТ-815	
АВТ-209	АВТ-112	АВТ-012	АВТ-941	АВТ-818	
АВТ-210	АВТ-113	АВТ-013	АВТ-942	АВТ-819	
АВТ-212	АВТ-114	АВТ-018	АВТ-943	АИ-82	
АВТ-213	АВТ-118	АВТ-019	АИ-92	АО-82	
АВТ-214	АВТ-119	АВТ-042	АО-91	АТ-83	
АВТ-218	АВТ-141	АВТ-043	АО-92	АТ-84	
АВТ-219	АВТ-142	АИ-02	АП-926		
АВТ-241	АВТ-143	АО-02	АТ-93		
АВТ-242	АИ-12	АП-026	АТ-94		
АВТ-243	АО-11	АП-027			
АВТ-244	АО-12	АТ-03			
АИ-22	АП-126	АТ-04			
АО-21	АП-127				
АО-22	АТ-13				
АП-226	АТ-14				
АП-227	АТ-15				
АТ-23					
АТ-24					
АТ-25					

Рисунок 4. Расписание занятий

Отчисление из НГТУ

Обучающийся может быть отчислен из НГТУ за академическую неуспеваемость, за дисциплинарные нарушения (в соответствии с уставом и правилами внутреннего распорядка НГТУ), по собственному желанию или по уважительной причине. Уважительной причиной является болезнь обучающегося, болезнь родственников и прочие обстоятельства, подтвержденные соответствующим документом.
За академическую неуспеваемость по представлению декана факультета приказом ректора (проректора) отчисляется обучающийся, имеющий 3 неудовлетворительные оценки за сессию (в том числе «незачеты») и не ликвидировавший академические задолженности в установленный срок (основание — Положение об экзаменах и зачетах).

Восстановление в НГТУ

Для восстановления обучающемуся необходимо предоставить в деканат документы:

- заявление на имя ректора, в котором указываются причина и год отчисления;
- справку о периоде обучения (академическую справку);
- документ об образовании, полученный при отчислении.

Восстановление обучающегося в НГТУ, отчисленного из НГТУ по собственному желанию или по уважительной причине, возможно в течение 5 лет после отчисления с сохранением основы обучения (бюджетной или контрактной) при наличии свободных мест. После восстановления студента на бюджетную основу обучения общий срок его обучения на бюджетной основе не должен превышать установленного времени обучения более чем на один год, а если студент также брал академический отпуск – не более чем на 2 года.

Восстановление обучающегося, отчисленного за академическую неуспеваемость, возможно с оплатой обучения.
Все остальные вопросы, связанные с восстановлением, решаются деканом факультета.

Положение о порядке перевода обучающихся из других вузов в НГТУ, из НГТУ в другие вузы, восстановления и перехода с одной образовательной программы на другую в НГТУ (файл pdf, 2,5 Мб).

Рисунок 5. Отчисление и восстановление

Рисунок 6. Каталог электронной библиотеки

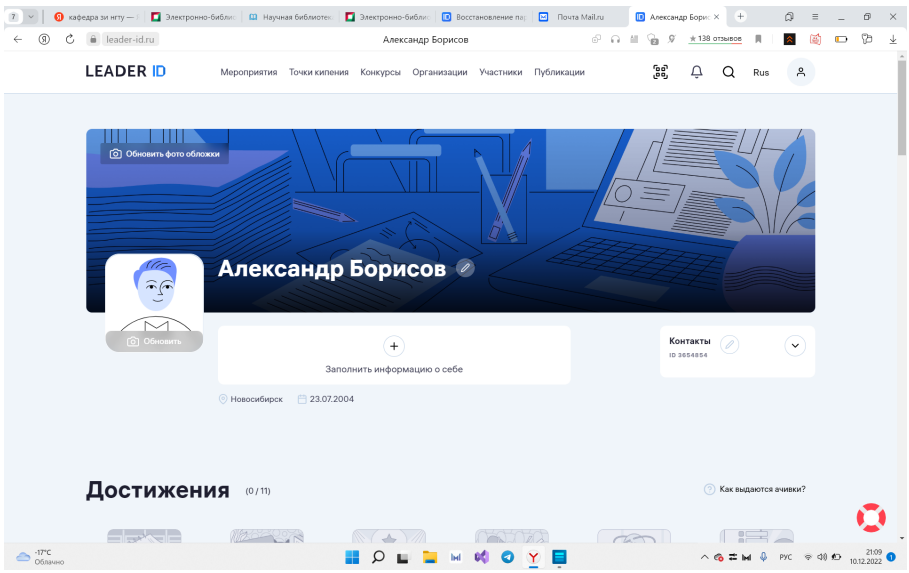


Рисунок 7. Регистрация на Leader-id

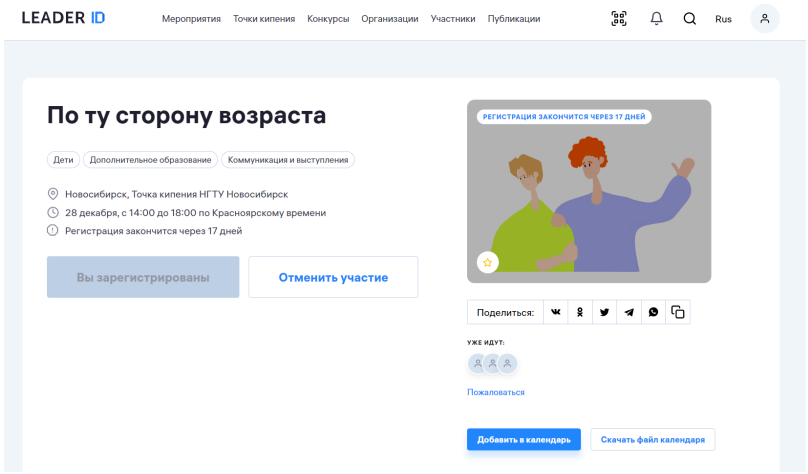


Рисунок 8. Регистрация на мероприятие

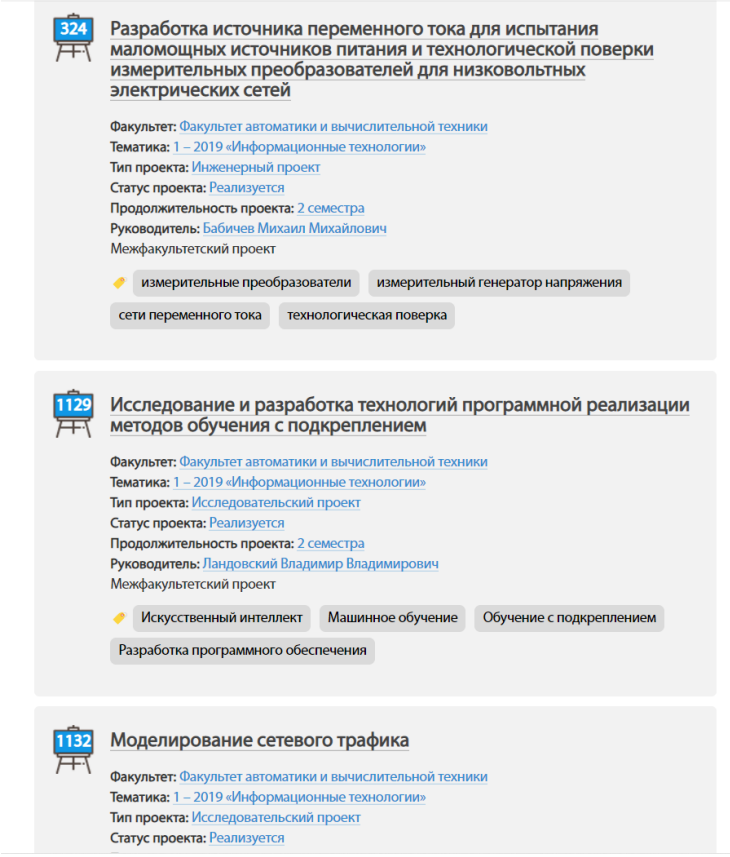


Рисунок 9. Проектная деятельность

Наиболее интересным проектом я считаю проект “Моделирование сетевого трафика”.

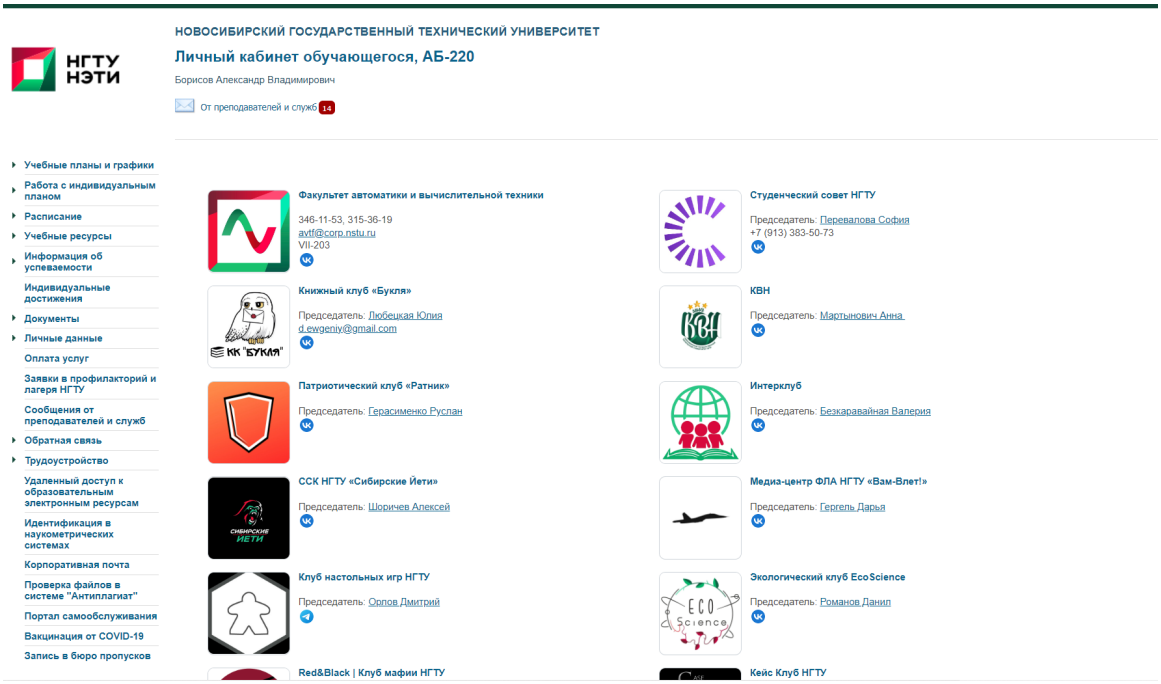


Рисунок 10. Личный кабинет обучающегося

2. Основные сведения

SIEM появился, когда компании обнаружили, что тратят много денег на системы обнаружения/предотвращения вторжений (IDS/IPS). Эти системы были полезны при обнаружении внешних атак, но из-за зависимости от механизмов, основанных на сигнатурах, было сгенерировано большое количество ложных срабатываний. Технология SIEM первого поколения была разработана для снижения этого отношения сигнал/шум и помогла выявить наиболее важные внешние угрозы. Используя корреляцию на основе правил, SIEM помог ИТ-отделу обнаруживать реальные атаки, сосредоточив внимание на подмножестве событий брандмауэра и IDS/IPS, которые нарушали политику. Традиционно SIEM-решения были дорогостоящими и отнимали много времени на обслуживание и настройку, но они решают большую головную боль, связанную с сортировкой чрезмерных ложных оповещений, и эффективно защищают компании от внешних угроз. Хотя это был шаг в правильном направлении, мир стал более сложным, когда новые правила, такие как Закон Сарбейнса-Оксли и Стандарт безопасности данных в индустрии платежных карт, привели к гораздо более строгому внутреннему ИТ-контролю и оценке. Чтобы удовлетворить этим требованиям, организации должны собирать, анализировать, составлять отчеты и архивировать все журналы для мониторинга действий внутри своих ИТ-инфраструктур.

Идея заключается не только в обнаружении внешних угроз, но и в предоставлении периодических отчетов о действиях пользователей и создании отчетов судебной экспертизы, связанных с данным инцидентом. Хотя технологии SIEM собирают журналы, они обрабатывают только подмножество данных, связанных с нарушениями безопасности. Они не были разработаны для обработки огромного объема лог-данных, генерируемых всеми ИТ-компонентами, такими как приложения, коммутаторы, маршрутизаторы, базы данных, брандмауэры, операционные системы, идентификаторы/IP-адреса и веб-прокси. С идеей отслеживать действия пользователей, а не внешние угрозы, log management вышла на рынок как технология с архитектурой для обработки гораздо больших объемов данных и возможностью расширения для удовлетворения потребностей крупнейших предприятий. Компании внедряют решения для управления журналами и SIEM для удовлетворения различных бизнес-требований, и они также обнаружили, что эти две технологии хорошо работают вместе. Инструменты управления журналами предназначены для сбора отчетов и архивирования большого объема данных журнала, в то время как решения SIEM предназначены для сопоставления подмножества данных журнала, чтобы указать на наиболее критические события безопасности.

При взгляде на корпоративный IT-арсенал можно увидеть как управление журналами, так и SIEM. Инструменты управления журналами часто выполняют роль хранилища данных журналов, которое фильтрует и пересылает необходимые данные журналов в SIEM-решения для корреляции. Такое сочетание помогает оптимизировать отдачу от инвестиций, одновременно снижая затраты на внедрение SIEM. В эти трудные экономические времена, скорее всего, компания попытается расширить свои технологии лесозаготовок, чтобы решить еще больше проблем. Он будет ожидать, что его технологии управления журналами и SIEM будут работать более тесно друг с другом и уменьшат дублирование функциональных возможностей.

Говоря простыми словами, SIEM - это система безопасности, состоящая из нескольких компонентов мониторинга и анализа, предназначенных для оказания помощи организациям в обнаружении угроз и их устранении.

Решения для управления информацией о безопасности и событиями представляют собой комбинацию двух различных продуктов, а именно SIM (управление информацией о безопасности) и SEM (управление событиями безопасности). Технология SIEM обеспечивает анализ предупреждений о безопасности, генерируемых сетевым оборудованием и приложениями, в режиме реального времени. Цель SIEM - помочь компаниям быстрее реагировать на атаки и упорядочить горы лог-данных. Решения SIEM поставляются в виде программного обеспечения, устройств или управляемых сервисов. Все чаще решения SIEM используются для регистрации данных о безопасности и создания отчетов в целях соответствия требованиям. Хотя информация о безопасности, средства управления событиями и ведения журналов дополняли друг друга в течение многих лет, ожидается, что эти технологии объединятся. Некоторые из других проблем, связанных с управлением журналами, включают устранение узких мест в сети, установление надежной передачи событий (например, системного журнала через UDP), установление требований к шифрованию и решение проблем с хранением необработанных данных. Итак, первыми шагами в этом процессе является определение того, какой тип журнала и информации о событиях необходимо собрать, как ее транспортировать и где хранить. Но это приводит к еще одному важному соображению о том, что один человек должен хотеть делать со всеми этими данными. Именно на этом этапе заканчивается базовое управление журналами и начинаются функции более высокого уровня, связанные с SIEM. Продукты SIEM обычно предоставляют многие функции, которые остаются необходимыми для управления журналами, но добавляют возможности уменьшения количества событий, оповещения и анализа в реальном времени. Они обеспечивают уровень технологии, который позволяет с уверенностью сказать, что журналы не только собираются, но и просматриваются. SIEM

также позволяет импортировать данные, которые не обязательно зависят от событий (например, отчеты о проверке уязвимостей), и это известно как “Информационная” часть SIEM.

Если отчетность о соблюдении требований является основной целью, то подумайте, каким правилам подчиняется компания. Часто компания подвергается многочисленным требованиям соответствия. Рассмотрим такую компанию и медицинского оборудования и программного обеспечения, они подпадают под действие HIPPA, как поставщик Министерства обороны, они подпадают под действие FISMA. Фактически, GE должна составлять отчеты о следующего поколения и управление журналами:

Одна из областей, где инструменты могут оказать наиболее необходимую помощь, - это соблюдение требований. Корпорации все чаще сталкиваются с проблемой сохранения подотчетности перед клиентами, сотрудниками и акционерами, а это означает защиту ИТ-инфраструктуры, клиентских и корпоративных данных и соблюдение правил и предписаний, определенных правительством и промышленностью. Соблюдение нормативных требований сохранится, и при администрации Обамы требования к корпоративной подотчетности, вероятно, будут расти.[3]

SIEM способна предоставить всю необходимую доказательную базу, подходящую для внутренних расследований инцидентов с утечкой данных. На самом деле, это одна из его главных целей. Во время инцидента все заинтересованные стороны будут проинформированы.

В настоящее время банковскому сектору больше всего нужны SIEM-системы, потому что:

а) они должны регулярно проводить проверки соответствия.

б) банки работают с конфиденциальной информацией, поэтому в случае инцидентов важно знать, кто-когда-откуда-куда просочился, был ли он злонамеренным или случайным и каковы были сопутствующие факторы.

Что касается бизнес-сферы, хороший инструмент SIEM может обеспечить аналитику, а знания хорошего инженера по безопасности могут быть автоматизированы и повторены в отношении множества событий с различных устройств. Вместо 1000 событий в день инженер с инструментом SIEM может обрабатывать 100 000 событий в день (или больше). И СИЕМ не уходит ночью, не находит другую работу, не делает перерыв или не берет отпуск. Это будет работать всегда.

Другая категория потребителей-это крупные предприятия (или географически распределенные предприятия), которые ежедневно генерируют множество событий с

различными свойствами и которые просто физически не отслеживаются, а менеджеры хотят "держать руку на пульсе", чтобы быстро реагировать на возможные инциденты.[4]

3. Архитектура

Обычно, SIEM-система разворачивается над защищаемой информационной системой и имеет архитектуру «источники данных» — «хранилище данных» — «сервер приложений». СИЕМ-решения представляют из себя интегрированные устройства (all-in-one) либо двух-трехкомпонентные комплексы. Распределеннная архитектура чаще всего предполагает большую производительность и лучшие возможности по масштабированию, а также позволяет развернуть SIEM-решение в IT-инфраструктурах с несколькими площадками.

Агенты выполняют первоначальную обработку и фильтрацию, а также сбор событий безопасности.

Передача информации от источников данных может осуществляться несколькими способами:

1. Источник сам инициирует передачу событий (например, отправляет по syslog-протоколу);
2. События с источника забираются пассивно.

С первым вариантом все довольно просто: источник указывает IP адрес устройства, собирающего события, события отправляются получателю. Второй вариант включает агентный или безагентный сбор данных, и в некоторых системах оба метода доступны в интернете для некоторых источников. Метод агента включает использование выделенной программы агента, метод без агента включает настройки источника событий, такие как создание дополнительных учетных записей, разрешение удаленного доступа и/или использование дополнительных протоколов.

Собранная и отфильтрованная информация о событиях безопасности поступает в хранилище данных, где хранится во внутреннем формате представления для последующего использования и анализа сервером приложений.

Сервер приложений реализует основные функции защиты данных. Он анализирует информацию со склада и преобразует её в генерацию предупреждений или управленческих решений о защите данных.

Исходя из этого, в SIEM-системе выделяются следующие уровни ее построения:

1. Сбор данных: осуществляется от источников различных типов, например, файловых серверов, межсетевых экранов, антивирусных программ. Сборщики выпускаются самых разных форм и размеров - от агентов, работающих на

контролируемом устройстве, до централизованных устройств регистрации с предпроцессорами для разделения потока данных. Это могут быть простые приложения для анализа файлов регулярных выражений или сложные агенты. Кроме того, поскольку данные системного журнала не зашифрованы, для обеспечения зашифрованной транспортировки может потребоваться сборщик;

2. Управление данными: данные, хранящиеся в репозитории, выдаются по запросам моделей анализа данных. На уровне презентации консоль представит события сотрудникам службы безопасности и менеджерам. Это основной интерфейс к системе для повседневных операций, и он должен эффективно расставлять приоритеты и представлять события с полной историей и обоснованием корреляции;

3. Анализ данных: результатом являются отчеты в предопределенной и произвольной форме, оперативная корреляция данных о событиях, а также выдаваемые предупреждения. Механизм анализа угроз должен будет работать в режиме реального времени, непрерывно обрабатывая и сопоставляя интересующие события, передаваемые ему сборщиком, и сообщая об обнаруженных угрозах консольному приложению или приложению уровня представления. Обычно для оперативных соображений достаточно сообщать о событиях, произошедших в течение 30 дней. Менеджеру журналов потребуется хранить большой объем данных, и он может использовать либо необработанные журналы, либо отфильтрованные интересующие события, а также сжимать, хранить и индексировать данные для долгосрочного криминалистического анализа и отчетности о соответствии требованиям. [5]

4. Функционирование систем

Знать потребность в инструменте SIEM в организации очень важно. Независимо от того, насколько хорош инженер по безопасности, около 1000 событий в день - это практический максимум, с которым инженер по безопасности собирается иметь дело. Поэтому, если команда безопасности хочет оставаться небольшой, она должна быть оснащена хорошим инструментом SIEM. Независимо от того, насколько хорошо работает отдельное устройство, если его не отслеживать и не коррелировать, каждое устройство можно обойти по отдельности, и общие возможности безопасности системы не превысят ее самого слабого звена. При мониторинге в целом, с корреляцией между устройствами, каждое устройство будет подавать сигнал тревоги при атаке, повышая осведомленность и указывая на угрозу в каждой точке, позволяя задействовать дополнительные средства защиты и реагировать на инцидент пропорционально общей угрозе. Даже некоторые представители малого и среднего бизнеса, имеющие всего несколько устройств, видят более 100 000 событий в день.

Самой большой проблемой при сборе данных в контексте SIEM является преодоление разнообразия форматов журналов. Система SIEM по самой своей природе будет извлекать данные из большого количества уровней — серверов, брандмауэров, сетевых маршрутизаторов, баз данных — и это лишь некоторые из них, каждый из которых регистрируется в другом формате.

Для решения поставленных задач SIEM-системы первого поколения применяют нормализацию, фильтрацию, классификацию, агрегацию, корреляцию и приоритезацию событий, а также генерацию отчетов и предупреждений. В SIEM-системах нового поколения к их числу следует добавить также анализ событий, инцидентов и их последствий, а также принятие решений и визуализацию.[6]

4.1 Функциональность

Агрегация данных: Представляя собой исходные данные запущенных процессов в цифровой среде, журналы являются идеальным источником для предоставления точной картины происходящего в режиме реального времени.

Независимо от того, создаются ли журналы брандмауэра, журналы сервера, журналы базы данных или любого другого типа, например, журналы SIEM, создаваемые в вашей среде, SIEM-системы способны собирать эти данные и хранить их в одном центральном месте для длительного хранения. Этот процесс сбора обычно выполняется агентами или приложениями, развернутыми в контролируемой системе и настроенными для пересылки данных в центральное хранилище данных SIEM-системы.

Корреляция: После сбора, анализа и хранения следующий шаг в системах SIEM отвечает за соединение точек и корреляцию событий из разных источников данных. Эта корреляционная работа основана на правилах, которые либо предоставляются различными инструментами SIEM, предопределены для разных сценариев атак, либо созданы и доработаны аналитиком. Проще говоря, правило корреляции определяет конкретную последовательность событий, которые могут указывать на нарушение безопасности. Например, можно создать правило для определения того, когда с определенных диапазонов IP и портов отправляется более x запросов в течение определенного промежутка времени. Объем данных, регистрируемых в средах, огромен. Даже небольшие и средние организации, скорее всего, будут отправлять десятки гигабайт данных в день. По сути, правила помогают сконденсировать эти данные в более управляемые наборы данных, устраняя шум и указывая на события, которые потенциально могут что-то значить. Корреляция, основанная на риске, может значительно сократить количество правил, необходимых для эффективной идентификации угрозы. Профили угроз и целей выполняют большую часть работы. Если атаки классифицированы по степени риска, три относительно простых правила корреляции могут идентифицировать более 99% атак.

Оповещение: автоматизированный анализ коррелирующих событий и генерация оповещений (тревог) о текущих проблемах. Оповещение может выводиться на «приборную» панель самого приложения, так и быть направлено в прочие сторонние каналы: e-mail, GSM-шлюз и т.п.

Инструменты отображения (информационные панели): Возможность визуализации данных и событий является еще одним ключевым компонентом систем SIEM, поскольку позволяет аналитикам легко просматривать данные. Все операционные системы, устройства и приложения генерируют своего рода журналы, содержащие системные события и уведомления. Информация в журналах может отличаться по общей полезности, но прежде чем можно будет извлечь большую пользу из них сначала их нужно включить, затем транспортировать и в конечном итоге хранить. Поэтому способ сбора этих данных из часто распределенных систем и передачи их в централизованное расположение является первой задачей управления журналами, которая имеет значение. Существуют различные методы достижения централизации, начиная от стандартизации механизма системного журнала и последующего развертывания централизованных серверов системного журнала до использования коммерческих продуктов для решения проблем сбора, транспортировки и хранения данных журнала.

Интероперабельность (трансформируемость): применение приложений автоматизации сбора данных, создание отчетов для адаптации агрегированных данных к существующим процессам управления информационной безопасностью и аудита.

Хранение данных: применение долгосрочного хранения данных в историческом порядке для сопоставления данных с течением времени и достижения возможности преобразования. Долгосрочное хранение данных имеет важное значение для проведения компьютерно-технических проверок, поскольку маловероятно, что расследование онлайн-инцидента будет проведено в самый момент нарушения. ИТ-организации также ожидают, что технологии управления журналами и аналитики обеспечат большую ценность для мониторинга деловой активности и бизнес-аналитики. Хотя SIEM продолжит собирать данные, связанные с безопасностью, его механизм корреляции может быть переназначен для корреляции бизнес-процессов и мониторинга внутренних событий, связанных с производительностью, временем безотказной работы, использованием возможностей и управлением уровнем обслуживания. Мы увидим, что объединенные решения обеспечивают более глубокое понимание не только ИТ-операций, но и бизнес-процессов. Например, мы можем отслеживать бизнес-процессы от шага А до Я, и, если какой-то шаг будет пропущен, мы увидим, где и когда. Короче говоря, интегрируя SIEM и управление журналами, легко увидеть, как компании могут сэкономить, отказавшись от дублирования усилий и функциональности. Функции сбора, архивирования, индексации и корреляции данных журнала могут быть свернуты. Это также приведет к экономии необходимых ресурсов и технического обслуживания инструментов.

Экспертный анализ: возможность поиска во многих журналах на разных узлах; это может быть выполнено в рамках программно-технической экспертизы.

5. Современные SIEM'ы

Согласно исследованию Garther, в число лидеров в 2018 году вошли следующие системы: Splunk, IBM и LogRhythm. Приведем их краткую характеристику:

Платформа SIEM от IBM является одной из самых передовых на рынке: даже в секторе лидеров Gartner она опережает конкурентов и успешно работает там уже 10 лет. Продукт состоит из нескольких интегрированных между собой систем, которые в совокупности обеспечивают максимальный охват событий, происходящих в сети, а многие функции работают непосредственно из коробки. Инструмент может собирать данные из различных источников, например, операционных систем, устройств безопасности, баз данных, приложений и многих других.

QRadar Security Intelligence может сортировать события по приоритету и выделять те, которые представляют наибольший риск для безопасности. Это связано с функциями анализа аномального поведения объектов (пользователей, оборудования, сервисов и процессов в корпоративной сети). В частности, определяются действия, связанные с доступом к подозрительным IP-адресам или запросам с них. Подробные отчеты предоставляются по всем подозрительным действиям, что, например, позволяет обнаруживать подозрительные действия в нерабочее время. Подобный подход в сочетании с функциями мониторинга пользователей и визуальным представлением сети на уровне приложений позволяет бороться с инсайдерскими угрозами. Кроме того, при обычных кибератаках информация поступает очень быстро и помогает предотвратить их до того, как они достигнут своих целей и нанесут значительный ущерб.

Обнаружение на основе рисков и определение приоритетов с использованием расширенного анализа и корреляции между активами, пользователями, сетевой активностью, уязвимостями, анализом угроз и т.д. являются основными функциями IBM QRadar Security Intelligence. IBM QRadar может объединять события в цепочку, создавая отдельный процесс для каждого инцидента. Благодаря тому, что информация собирается и отображается на экране в одном месте, администратор может видеть все связанные с этим подозрительные действия, обнаруженные системой. И новые связанные события добавляются в единую цепочку, поэтому аналитикам не следует переключаться между несколькими оповещениями. А для более глубоких расследований специальный инструмент IBM QRadar Incident Forensics может восстановить все сетевые пакеты, связанные с инцидентом, и пошагово воссоздать действия злоумышленника.

Splunk — это еще одно решение для ведения коммерческих журналов событий. Благодаря веб-интерфейсу Splunk интуитивно понятен в настройке и управлении. Splunk использует достаточно удобный для пользователя подход к проектированию интерфейсов,

упрощая первоначальный опыт для менее опытного администратора. Как и у многих аналогичных продуктов для ведения журналов, возможность создания отчетов является частью базового продукта и, в случае Splunk, она относительно проста в использовании. Распространенные типы форматов представления данных доступны из раскрывающихся меню на экране. Одна из приятных сторон веб-интерфейса Splunk заключается в том, что любой отчет может быть предоставлен в виде URL-адреса, что позволяет другим людям в организации просматривать конкретные отчеты, которые системный администратор создает для них.

LogRhythm, Inc. — американская компания, занимающаяся вопросами безопасности, которая объединяет систему управления информацией и событиями безопасности (SIEM), управление журналами, мониторинг сети и конечных точек, а также аналитику и безопасность. LogRythm нацелен на обеспечение автоматизации и соответствия нормативным требованиям. Продукты LogRhythm призваны помочь организациям защитить свои сети и оптимизировать работу. Кроме того, они помогают автоматизировать сбор, организацию, анализ, архивирование и восстановление данных журналов, что позволяет компаниям соблюдать правила хранения данных журналов. Компоненты продукта включают в себя сбор данных, мониторинг системы и сети, аналитические модули, управление журналами и событиями.[7]

В последнее время на рынке появляются отечественные решения, среди которых:

Security Capsule — первая Российская система контроля за информационной безопасностью. Является самой доступной среди применяемых в России SIEM - систем. Обладает следующими качествами: выявление сетевых атак как в локальных, так и в глобальных периметрах, обнаружение вирусных заражений, способность регистрировать события в используемой операционной системе, учёт действий лиц, взаимодействующих с системой управления базой данных.

MaxPatrol SIEM — система, имеющая объективную оценку уровня защищённости как отдельно взятых подразделений, узлов и приложений, так и всей системы в целом. В сравнении с выше рассмотренным программным продуктом выделяется более высокой стоимостью. Данная система характеризуется использованием эвристических механизмов анализа и сформированной базой знаний, способной осуществлять проверку большинства распространённых операционных систем и специализированной аппаратуры. В отличие от классических SIEM-систем, она не нуждается в установке программных компонентов на узлах, что существенно облегчает процесс использования и снижает конечную стоимость владения. Обладает легко настраиваемой системой и разграничением прав доступа, что даёт возможность формировать мониторинг ИБ на каждом из уровней иерархии. Для

отдельно взятого пользователя MaxPatrol, присутствует возможность создать свой список задач, которые он способен выполнить внутри системы.[8]

RUSIEM — по замыслу разработчиков, продукт должен заменить зарубежные аналоги на российском рынке и вести с ними конкурентоспособную борьбу за счёт невысокой стоимости внедрения и поддержки, а также мощной функциональности. Видимыми отличиями от конкурирующих компаний являются: интерпретирование событий в понятный вид, тегирование и весовые показатели, что даёт более удобный и быстрый способ анализировать поступающую информацию. Также стоит отметить безлимитное количество источников информации, что вкупе с компактным хранилищем даёт возможность строить оптимизированные запросы на любой глубине хранилища.[9] [10]

Заключение

В ходе учебной практики мы изучили навигацию на сайте НГТУ и электронных ресурсах DiSpace, YourNETI, Leader-ID; познакомились с кафедрой Защиты информации НГТУ НЭТИ; выяснили, что SIEM - это сложная технология, и сегмент рынка остается изменчивым. Решения SIEM требуют высокого уровня технической экспертизы, а поставщики SIEM требуют обширной подготовки партнеров и сертификации. SIEM становится более захватывающим, когда можно применять данные об активности на основе журналов и корреляцию, основанную на событиях безопасности, к другим бизнес-задачам. Соблюдение нормативных требований, мониторинг деловой активности и бизнес-аналитика - это лишь верхушка айсберга. Передовые клиенты уже используют инструменты для повышения видимости и безопасности составных приложений Web 2.0, облачных сервисов и мобильных устройств. Ключ в том, чтобы начать с централизованного учета активности пользователей и системы и построить открытую архитектуру, которая позволяет различным бизнес-пользователям получать доступ к информации для решения различных бизнес-задач. Таким образом, нет никаких сомнений в том, что SIEM-решения помогают улучшить обнаружение вторжений и реагирование на них.

В целом, количество IT-специалистов и специалистов, ориентированных на безопасность, в любой конкретной компании сократилось по сравнению со сложностью и возможностями, требуемыми все более взаимосвязанной сетью. В то время как в одном решении могут работать десятки высококвалифицированных инженеров по безопасности, просматривающих отдельные журналы событий для выявления угроз, SIEM пытается автоматизировать этот процесс и может добиться законного сокращения более чем на 99,9% данных о событиях безопасности, в то время как это фактически повышает эффективность

обнаружения по сравнению с традиционным мониторингом, управляемым человеком. Вот почему SIEM предпочитают большинство компаний.

Кроме того система может:

- Анализировать события и создавать алерты при каких-то аномалиях: сетевого трафика, неожиданных действий пользователя, неопознанных устройствах и т.д.
- Проверить на соответствие стандартам (PCI DSS, COBIT и др). Не без подводных камней, правда.
- Создать красивый отчет. В том числе настроенный непосредственно для ваших нужд. Например, ежедневный отчет об инцидентах, еженедельный отчет нарушителей, отчет по работоспособности устройств и т.д. Отчеты настраиваются гибко, как и их получатели.
- Мониторить события от устройств/серверов/критически важных систем, создавать соответствующие оповещения для заинтересованных лиц.
- Собрать доказательную базу по инцидентам.

Технологии управления журналами и корреляции SIEM могут работать вместе, чтобы обеспечить больше

всесторонние представления, помогающие компаниям выполнять свои нормативные требования, повышать эффективность своих ИТ- и бизнес-процессов и снижать затраты на управление и технологии в процессе.

требований по крайней мере для одного корпоративного подразделения практически по каждому нормативному акту.

Список источников

1. Кафедра защиты информации [Электронный ресурс] https://ciu.nstu.ru/kaf/zi (дата обращения: 08.12.2022)
2. Новосибирский государственный технический университет [Электронный ресурс]. https://www.nstu.ru/. (дата обращения: 08.12.2022)
3. Microsoft security. Общие сведения о SIEM-системах [Электронный ресурс] https://www.microsoft.com/ru-ru/security/business/security-101/what-is-siem (дата обращения: 09.12.2022)
4. Что такое SIEM [Электронный ресурс] https://www.securitylab.ru/analytics/430777.php (дата обращения: 09.12.2022)
5. SIEM и (или) сканер уязвимостей [Электронный ресурс] https://www.securitylab.ru/analytics/430782.php (дата обращения: 09.12.2022)
6. Энциклопедия Касперского [Электронный ресурс] https://encyclopedia.kaspersky.ru/glossary/siem/ (дата обращения: 09.12.2022)
7. Обзор решений SIEM (Security information and event management) [Электронный ресурс] https://habr.com/ru/company/roi4cio/blog/528770/ (дата обращения: 10.12.2022)
8. MaxPatrol SIEM - выявление инцидентов информационной безопасности от Positive technologies. [Электронный ресурс] https://www.ptsecurity.com/ru-ru/products/mpsiem/ (дата обращения: 10.12.2022)
9. Обзор систем SIEM на мировом и российском рынке [Электронный ресурс] https://www.anti-malware.ru/analytics/Technology_Analysis/Overview_SECURITY_systems_global_and_Russian_market (дата обращения: 10.12.2022)
10. Алексей Парфентьев, “СёрчИнформ”, о SIEM и вреде лишних фич. - Журнал “Хакер”, выпуск от 26.11.202 (дата обращения: 09.12.2022)

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Новосибирский государственный технический университет»

Кафедра _Защиты информации_____

ДНЕВНИК ПРОХОЖДЕНИЯ ПРАКТИКИ

Наименование практики: Учебная практика: ознакомительная практика_____

_____

Направление подготовки: 10.03.01 Информационная безопасность_____

_____

Студент _____Борисов А. В._____

(Ф. И. О.)

Группа _____АБ-220___

Факультет _____АВТФ_____.

Новосибирск 2022

Индивидуальное задание на практику

Задачи практики:

Вопросы, подлежащие изучению

На подготовительном этапе:

1) Регистрация в личном кабинете НГТУ
2) Установка приложения YourNETI
3) Регистрация на DiSpace
4) Регистрация на Leader.id

На основном этапе:

1) Ознакомление с учебными лабораториями и профессорско-преподавательским составом кафедры ЗИ
2) Ознакомление с возможностями навигации на сайте НГТУ
3) Ознакомиться с содержанием электронной научной библиотеки
4) Ознакомиться с функционалом среды дистанционного обучения DiSpace
5) Найти интересующее ближайшее мероприятие в точке кипения НГТУ либо академпарка
6) На сайте НГТУ открыть личный кабинет студента
7) Изучить возможности приложения YourNETI

На итоговом этапе:

1) Оформление отчета по практике
2) Защита отчета по практике

Ожидаемые результаты практики:

1) Ознакомление с функциональными сервисами НГТУ

2) Изучение правил написания отчетов и рефератов

3) Ознакомление со специальностью путем прослушивания лекций по учебной практике

4) Изучение выбранной для реферата темы более углубленно

Календарный график выполнения задания на практику

Дата	Наименование работ	Отметка руководителя о выполнении задания
01.09	Регистрация в личном кабинете НГТУ и DiSpace	
03.09	Скачивание и ознакомление с приложением YourNETI	
12.09	Лекция №1. Презентация группы компаний ООО “СИБ”; рассказ П. Мартенса о CTF	
26.09	Лекция №2. Презентация компании Positive Technologies; Презентация “Управление ФСТЭК России по СФО”	
10.10	Лекция №3. Презентации компаний Astra linux и ЦФТ	
24.10	Лекция №4. Презентации компаний Eltex, UserGate, Infotecs	
21.11	Лекция №5. Технические каналы управления информацией	
29.11	Регистрация на leader-id	
01.12	Ознакомление с содержанием электронной научной библиотеки	
03.12	Ознакомление с возможность участия в проектной деятельности	
06.12	Изучение основного функционала приложения YourNETI	
10.12	Оформление отчета по уч. практике	
_.12	Защита отчета по практике	

Студент группы _____АБ-220_____

Ф. И. О. _____Борисов А. В._____ Подпись 

Дата 10.12.2022

Руководитель практики:

От НГТУ НЭТИ:____Иванов А. В._____ к.т.н., доцент кафедры ЗИ НГТУ

(Ф. И. О.) *(должность)*

Задание принято к исполнению:  «___» _____ 201_ г.

(подпись студента)