Общество с ограниченной ответственностью «МультиТек Инжиниринг»

Программный комплекс по обучению, тренировке навыков и контролю знаний сотрудников по информационной безопасности



Минск 2021

Содержание

1.	Общие сведения	3
2.	Назначение, условия применения и поставки Системы	4
3.	Функции Системы	5
4.	Архитектура Системы	6
5.	Настройка Системы	7
6.	Подготовка шаблонов для атак	12
7.	Подготовка новой атаки	14
8.	Выполнение учебных атак и тренировка навыков	15
9.	Результаты учебных атак	19
10.	Формирование рейтинга	19
11.	История действий	20
12.	Обучение сотрудников	21
13.	Работа со статистикой и отчётами	27



1. Общие сведения

Данный документ содержит описание Программного комплекса по обучению, тренировке навыков и контролю знаний сотрудников по информационной безопасности «Антифишинг» (далее – Система, «Антифишинг»).

Цель документа – предоставить заинтересованным предприятиям и организациям (далее – заказчики) информацию, позволяющую сделать осознанный выбор решения для обеспечения требуемого уровня осведомленности и навыков безопасной работы сотрудников.

Разработчиком Системы является ООО «Антифишинг» – российская исследовательская компания и разработчик программного обеспечения.

ООО «Антифишинг» (далее – производитель) работает на рынке с 2016 года, специализируясь на решении проблем человеческого фактора в информационной безопасности. В штате компании – специалисты по практической безопасности, разработчики, тестировщики, аналитики, психолог, редакторы и методологи.

Производитель ведёт собственные исследования, развивает уникальную классификацию цифровых атак на людей и поддерживает её в «Антифишинге».

ООО «МультиТек Инжиниринг» является официальным партнером ООО «Антифишинг» в Республике Беларусь, имеет в штате обученных специалистов, что позволяет обеспечить высокое качество настройки, интеграции и технической поддержки Системы.

При возникновении вопросов по Системе, не нашедших отражение в настоящем документе, а также при желании провести пилотный проект Системы, необходимо направить электронное письмо на адрес info@mte-cyber.by.



2. Назначение, условия применения и поставки Системы

«Антифишинг» предназначен для автоматизации следующих процессов:

- обучение сотрудников основам информационной безопасности;
- контроль уровня знаний сотрудников;
- тренировка и формирование навыков безопасной работы;

• отслеживание уязвимостей в клиентских приложениях (операционных системах, браузерах, офисных пакетах) с привязкой к небезопасным действиям и выдача рекомендаций по устранению уязвимостей.

В настоящем документе рассматривается «Антифишинг» в исполнении On Premise STANDARD, работающий внутри периметра безопасности заказчика.

Система предоставляет возможность интеграции с системами обучения WebTutor и Moodle и позволяет, помимо использования собственных обучающих курсов, загружать любые курсы обучения в виде SCORM-пакетов.

Панель мониторинга («дашборд») Системы позволяет отслеживать, как изменяются знания и навыки сотрудников. Кроме того, всем сотрудникам, подразделениям и заказчику в целом присваивается рейтинг в зависимости от безопасности их действий.

Система лицензируется по количеству пользователей (минимальное количество – 300) и сроку применения. Возможна поставка лицензии на 1 год или на несколько лет.

В стоимость лицензии «Антифишинга» включены стоимость работ по адаптации курсов по требованиям политик безопасности заказчика, брендирование и замена контактной информации, а также стоимость технической поддержки.

Система поставляется в подготовленном к настройке состоянии в виде виртуальной машины с установленной операционной системой CentOS 7.

Минимальные технические требования к серверу:

- 2 CPU;

- 4 Гбайт RAM;
- 60 Гбайт HDD.

Весь контент, а также интерфейсы Системы доступны на русском, английском и итальянском языках.



3. Функции Системы

Система обеспечивает:

- автоматизацию процессов обучения и контроля защищённости сотрудников;
- имитацию целевых атак через электронную почту, ссылки, вложения различных типов, фишинговые сайты и USB-устройства;
- возможность создания заказчиком собственных шаблонов атак;
- проведение имитаций атак по различным технологическим и психологическим векторам;
- контроль уровня осведомлённости и уровня навыков сотрудников;
- контроль уязвимостей приложений;
- собственные электронные курсы и их бесплатную адаптацию под требования заказчика;
- регулярные обновления материалов для обучения и тренировки навыков;
- использование планировщика для полной автоматизации процессов;

ООО «МультиТек Инжиниринг»

– АРІ для интеграции с другими процессами и системами безопасности.



4. Архитектура Системы

Система состоит из следующих основных компонент:

- Attack компонент тренировки навыков (отправка атак);
- Edu компонент управления обучением (прохождение курсов обучения и сдача зачетов);
- Mail внутренний почтовый сервер (отправка уведомлений об обучении и имитированных атак).

Общая схема работы Системы представлена на рис.1.



Рисунок 1. Общая схема работы Системы



5. Настройка Системы

Для того, чтобы начать работу, необходимо войти в консоль администрирования (административный интерфейс) Системы (рис. 2).



Рисунок 2. Консоль администрирования

Консоль администрирования предлагает следующие возможности:

- раздел «Знания»: отслеживание уровня знаний сотрудников, создание новых учебных атак;
- раздел «Навыки»: отслеживание навыков сотрудников, запуск учебных атак;
- раздел «Рейтинг»: отображение рейтинга по сотрудникам и отделам, вся отчётность;
- раздел «Уязвимости»: выявление программных брешей в пользовательских приложениях на основе небезопасных действий сотрудников;
- раздел «Настройки»: определение всех параметров Системы;
- раздел «Планировщик»: автоматизация и управление задачами по расписанию.

Кроме того, предоставляется возможность просмотра на одной странице всех функций одновременно – путём нажатия на кнопку классического меню в верхнем левом углу.

Одновременно в Системе могут работать несколько сотрудников – менеджеры и специалисты по безопасности, аудиторы, HR-специалисты и



администраторы информационной безопасности.

Встроенная ролевая модель и многопользовательский режим позволяют назначить каждому сотруднику только необходимые права доступа (рис. 3).

Ант		Lizz (a Dana				me [+
: Знань	Новая роль					× 27%
Har	Название	Новая роль для млади	иего специалиста	no NE	Настройки	
	Страница по-умолчанию	сотрудники Атаки	уязвимости	Отчеты	пастроики	
Уч	Доступы	 Дэшборд Сотрудники (знания обърдоника и на 	i)			
фŀ		добавление и из удаление сотруд	чиков	ников		
фр Аң Мс		 создание атаки назначение обуч просмотр истори сохранение отчё сохранение отчё 	ения и та по действия та по обучению	N		
За		Атаки (навыки) Добавление и из	менение атак			
Ko		 удаление и восст планирование, з просмотр отчето 	ановление атан апуск и останов в по запускам а	ка атак так		
Po		🗌 Риски (уязвимости)				
на то Ад		 Отчёты (рейтинг) отчёты по атакая отчёты по отдел. сохранение общ полная статистия анонимная стати 	и ам его отчета ка стика			
То		🗌 Настройки				
		🗌 Учётные записи адя	иинистраторов			
Пл		🗌 Роли администрато	ров			
Ha		r				
00	Отменить Добавить	J				
				отчёт по	о рискам	_

Рисунок 3. Создание новой роли

В разделе «Знания» можно добавлять учётные записи сотрудников, группировать их в подразделения – как в ручном режиме, так и с помощью импорта из файла формата XLS, из Active Directory, через API (рис. 4).

Для более удобного отображения информации доступна сортировка по сотрудникам, отделам или руководителям. В дальнейшем можно назначать сотрудникам атаки и курсы обучения, просматривать историю действий сотрудников, удалять или изменять учётные записи.



Сотрудники - цели для атаки								
Добавить отдел	Добавить сотрудников			Выбрать всех	7	ФИО, почта ил	и рейтинг	Q
+1 по рейтингу	🛄 по обучению 🧳 по р	уководител	ю по отделам	общим списком				
ФИО↓	Электронная почта	Отдел	Должность	Текущий рейтинг		Активен	метки	
Москалёв Егор Сергеевич	e.mos@mte-cyber.by	ИБ	Системный архитектор	-1 20 открыл	письмо	734 дня	3.Третий	
Ременчик Владислав	v.remenchik@mte-cyber.by	ИБ	инженер	-4 2 🖉 епереше	л по ссь	ілке 1 день	1.Первый	

Рисунок 4. Отображение списка сотрудников в разделе «Знания»

В разделе «Навыки» отображаются подготовленные ранее учебные атаки (рис. 5). Здесь можно производить запуск этих атак сразу же или через заданный промежуток времени, используя планировщик.

Каждая атака размечается по атрибуции и психологическим векторам в соответствии с классификацией производителя.

Кроме того, есть возможность скопировать атаку и внести практически любые изменения в её шаблон. Отсюда же можно сохранять отчёты о проведённых тренировках.

Антифиши	H / Antiphishing for Demo		📰 🐯 support@antph.me [
Знания 14%	Навыки 10%	Рейтинг 8 ⁻¹¹	Уязвимости 29
Атаки на сотру	дников		
Электронная почта Съёмни	ые устройства 🕺 Создать атак	у	
Эвакуация 1 цель			~
Страх Желание помочь	Срочность Любопытство 🔀 Внешня	яя атака через 3 месяца	25 дек 2020 17:28
не запускалась			
Jira 1 цель			
Любопытство Раздражени	е Срочность 🔀 Внешняя атака		
отчеты за 14 октября			
Demo: Zoom initing	(ENG) 1 цель		
Страх Любопытство О	Брочность 🔀 Внешняя атака		

Рисунок 5. Список учебных атак в разделе «Навыки»

В разделе «Уязвимости» (рис. 6) можно посмотреть найденные проблемы и риски: бреши в операционных системах, браузерах, офисных пакетах, почтовых



клиентах и других приложениях, с которыми работают сотрудники и которые Система определяет, как уязвимые, анализируя актуальность версий и их обновлений.

Отчёт из этого раздела можно передавать коллегам для повышения приоритетов патч-менеджмента, а устранённые уязвимости можно отмечать – они исчезнут из этого представления.



Рисунок 6. Информация в разделе «Уязвимости»

Через раздел «Настройки» (рис. 7) задаются различные параметры Системы – учётные записи администраторов, конфигурация уведомлений и системы обучения, импорт из LDAP и другие.



Настройки			
Администратор	выход из системы	L	Лицензия
ΦΝΟ	Москалёв Егор Сергеевич		MTE / mte-cyber.by
Электронная почта	e.mos@mte-cyber.by	J	действует до 1 июля 2021
Телефон	+375445506905	٤	8 из 500 возможных сотрудников в системе
Часовой пояс	GMT+3 Europe/Minsk	l	
Отдел	ИБ	4 × (для изменения условий лицензии отправьте запрос на адрес support@antiphish.ru
Должность	Системный архитектор	E	Версия: 2.4.2 си11
	Создать как цель		
Старый пароль			
Новый пароль	Сгенерировать		
	Сменить пароль или Требования к паролю		

11

Рисунок 7. Перечень параметров лицензии из раздела «Настройки»

Планировщик позволяет автоматизировать процессы обучения и тренировки навыков, а также формирования и отправки отчётности. При этом можно создавать сложные конструкции с использованием логических элементов «и»/«или», а также планировать различные действия с задержкой по времени, сразу или с определённой частотой выполнения (рис. 8).

Новое правило		,	
Название			
Что случилось?	Выберите триггер	•	
	Открыл вложение 🔴		
Что нужно сделать?	Ввел данные в форму 🔵 Обнаружены уязвимости 🔵	\oplus	
	Выдержал атаку 🔵	1	
Выполнить	Сотрудник не был обучен 🅢		
	Назначен на обучение 🏈 Завершил обучение 🖉		
Отменить Сохранить	ana dia any amin'ny Kaodim-Paositra 🖉		

Рисунок 8. Пример триггеров планировщика — возможных состояний, на основе которых автоматизируются процессы

Производитель поставляет и в рамках технической поддержки на основе



методологии «Антифишинга» ежеквартально обновляет базовые правила (пример правила приведен на рис. 9), которые создаются с помощью планировщика.

Название	Отпра	вка атаки, е	сли вы	держал '	1 раз с заде	ержкой 2 недели
Что случилось?	Выдер	жал атаку				••
	однаж атака сч через 2	ды нескол читается вы 4 часа посл	лько р ідерж іе запу	аз подря анной п уска	ид ри отсутст	твии действий по ней
Что нужно сделать?	3anyci	гить атаку				• 🕀
	Случайный шаблон 👻					
	✓ не и Со со со Со со со С вло С фи	спользовал сылкой эжением шинговой (іся ра страні	нее ицей		
Выполнить	сразу	с задержко	рй	не чаще	, чем	
	2	минуты	часа	а дня	недели	

Рисунок 9. Пример правила в планировщике

6. Подготовка шаблонов для атак

Производитель в рамках технической поддержки занимается созданием шаблонов целевых атак для каждого заказчика.

Эта работа основана на собственных психологических и технических исследованиях, которые производитель проводит с 2017 года (собирает и публикует еженедельную аналитику по фишингу и другим цифровым атакам на людей, участвует в информационном обмене с ФинЦЕРТ Банка России и др.), что позволяет ему предлагать заказчикам самые актуальные целевые атаки (пример сценария атаки приведен на рис. 10) и обучающие материалы.



Сценарии соответствуют классификации Антифишинга

Ид	Сценарий	Вектора атаки	Технологии	
1	Письмо от вендора (радини сара), который <mark>предлагает провести обзор</mark> новой версии Web application firewall. Во вложении	Внешняя Персональная Любопытство	Эл. письмо Вложение MS Word	
	ReleaseNotes, компания	Menanie Homoris		
	тестирования в течение двух дней.			
2	Независимый эксперт отправляет статью для	Внешняя	Эл. письмо	
	публикации по теме "Влияние Искусственного	Анонимная	Вложение pdf	
	интеллекта на жизнь безопасника". Статья	Любопытство		
	находится во вложении.			
3	Письмо от Генерального директора, в котором	Корпоративная	Эл. письмо	
	он обращается к сотруднику по имени и	Персональная	Ссылка	
	требует срочно проверить, кто согласовал эту	Страх		
	новость на корпоративном сайте.	Срочность Авторитет		

4	Письмо от Госуслуг, в котором к сотруднику обращаются по имени, сообщают о	Личная Персональная	Эл. письмо Ссылка	
	правонарушении и приводят подробности (адрес недалеко от офиса, другие детали).	Раздражение <mark>Жадность</mark>	Фишинговая gosuslusi.ru	
	Там же указана сумма штрафа. Предлагается посмотреть подробности по ссылке и оплатить штраф со скидкой 50% до конца недели.	Срочность Авторитет		
5	Письмо от сотрудника, который просит срочно	Корпоративная	Эл. письмо	
	подключиться к его видеоконференции по	Персональная	Ссылка	
	ссылке (Zoom, Google Meet, Skype for	Желание помочь	•	
	business) для помощи по важному проекту.	Страх	Фишинговая ссылка	
	Фишинговая страница запрашивает доступ к камере.	Срочность Авторитет	Zoom/Google Meet/Skype for business	
6	Рассылка от информационной системы об	Корпоративная	Эл.письмо	
	учащении случаев мошенничества и	Анонимная	Ссылка	
	проведении профилактических мероприятий,	Страх	•	
	необходимо в ближайшее время сменить	Срочность Авторитет	Фишинговое окно блокировки ОС	

Рисунок 10. Пример сценария имитированных атак

После согласования сценария с заказчиком производитель разрабатывает шаблон атаки (в виде писем со всем оформлением: ссылками, вложениями, фишинговыми страницами) для внесения изменения в Систему.



7. Подготовка новой атаки

Для того, чтобы подготовить новую проверку, необходимо нажать на кнопку «Создать атаку»; появится окно для определения параметров.

В качестве примера выбран шаблон атаки от имени компании, которая приглашает работников на международный форум. (рис. 11).

	Ан-	МТЕ: Приглашение на г	международный форум	× er.bv F→
		Название	МТЕ: Приглашение на международный форум	
		Цели для атаки	3 цели Изменить список целей 🛛 😥	
Шаблон МТЕ: Приглашение на между			МТЕ: Приглашение на международный форум	×
			Все векторы Выбранные 🏌 Самые опасные	
	2 H			з имеют жений
			Внешняя атака Порпоративная Личная	
	Соті		Классификация атак Антифишинга 🖓	лействиям
	Добави	Тема письма	Приглашение на XVI Международный форум БАНКИТ	٩
	+1 по р Отдел	Отправитель	Малкина Алеся <a.malkina@infobark.by></a.malkina@infobark.by>	Людей
	ИБ	Адрес	a.malkina.infobark.by @ antph.ru •	8
	ФИО↓		Такой же в ссылках	етки
	Годун И Павлов	♠ ๗ Формат - В		третий
	Красни Давидо	Second name) (first name) anna		Первый
	Москал Сергеев	Пищу с тем, чтобы официально при (Президент отель). Мы будем очен мероприятия и вызовут интерес у с	стерите. игласить Вас на XVI Международный форум «БАНКИТ», который пройдет 22-24 октяб ь рады видеть Вас в качестве спикера и уверены, что ваш опыт и знания обогатят пр лушателей.	ря в Минске ограмму нашего
M	Ременч	Предлагаем выбрать тему и удобно спикеров, необходимо заблаговрем	е время выстуления. Во вложении <u>программа выступления</u> . Ввиду большого количес менно забронировать тему и временный слот.	тва планируемых
	Шильді Львови	Будем ждать ответа!		Гретий
	Шишко	С уважением,		второй
	Анатолі	Алеся Малкина.	ununun faranzunzu Hauma zavianaria	
M	Шпак В Игорев	лдминистратор комитета по инфор Тел: 200-64-44	мационной оезопасности научно-технологической ассоциации «Инфорарк»	второй
	Ruyopa	+ 375-44-54-777-91		
	Альбер	E-mail: <u>a.malkina@infobark.by</u>		

Рисунок 11. Создание новой учебной атаки

По классификации производителя у этой атаки будут следующие параметры:

- атрибуция: корпоративная атака; _
- психологические векторы и усилители: страх, авторитет, срочность;
- персонификация: есть. _



В зависимости от сценария в атаку могут добавляться файлы различных типов, фишинговые страницы и финальные страницы с обратной связью для пользователей (рис. 12).

тчеты :	П Вложение	Jpeg Zip	Release Notes_Continet.docx	• /
nti-N	Фишинговая страница	Проверять в ЦСо	Windows + Icon	•
Страх			Аутентификация Госуслуги	
c surry.	Финальная переадресация		Windows + Icon Microsoft Teams - Video2	

Рисунок 12. Внесение изменений в учебную атаку

После того как учебная атака будет создана и назначена сотрудникам, она отобразится в списке атак раздела «Навыки» (рис. 13).

Атаки на сотрудников

Электрон	ная почта (Съёмные устро	йства 🖇 Создать	атаку
Ново	ть на сай	йте	1 цель	Запустить атаку
Страх	Авторитет	Срочность	Корпоративная	
не запус	калась			

Рисунок 13. Подготовленная учебная атака на сотрудников

Атаку можно выполнить немедленно или в запланированный момент времени, а также удалить её либо скопировать, после чего внести в сделанную копию изменения (например, поменять текст письма, адрес и имя отправителя, тему, финальную страницу, вложение и т. д.).

8. Выполнение учебных атак и тренировка навыков

Атаки после запуска приходят сотрудникам, а Система фиксирует возможные небезопасные действия – загрузку внешнего содержимого, открытие файлов и отключение защищённого режима (для офисных документов), переходы по ссылкам и ввод паролей, или, например, разрешение на доступ к камере и микрофону (рис. 14).





Рисунок 14. Проведение учебной атаки через доступ к камере и микрофону

Как только сотрудник совершает небезопасное действие, Система показывает ему эмоциональную обратную связь и тут же объясняет, как нужно действовать безопасно в подобной ситуации.

Другая атака выглядит для пользователя как ошибка, которая появляется в операционной системе. Язык, текст и внешний вид ошибки адаптируются под операционную систему и действующие параметры пользователя (рис. 15).



Рисунок 15. Ложная ошибка в операционной системе



ООО «МультиТек Инжиниринг»

e-mail: info@mte-cyber.by

16

После нажатия на любой элемент окна экран пользователя блокируется (рис. 16) — вместо браузера и интерфейса операционной системы пользователь видит знакомый экран блокировки. Оформление, шрифты и другие параметры подбираются в соответствии с действующими групповыми политиками.



Рисунок 16. Экран блокировки рабочего стола в Системе

При попытке «разблокировать» компьютер пользователь видит свои имя и фамилию, адрес электронной почты и даже свою фотографию, если он авторизован на одном из популярных сайтов, которые проверяет производитель (рис. 17).



Рисунок 17. Ложное окно авторизации



ООО «МультиТек Инжиниринг»

e-mail: info@mte-cyber.by

Пароль может сверяться с действующим доменным паролем учётной записи пользователя, если в Системе включена синхронизация с LDAP, и администратор выбрал соответствующий пункт в параметрах атаки (рис. 18).

ti-N	🗹 Фишинговая страница	Проверять в LDAP	Windows + Icon	•
pax				

Рисунок 18. Включение синхронизации с LDAP

Также Система может фиксировать безопасное поведение сотрудников – например, умение выявить атаку и сообщить о ней через плагин в почтовом клиенте (рис. 19).

🧧 😑 🍳 🧧 🤝 🗇 🛱 🛛 Расчет заработной платы за текущий месяц - Temporary Items	
Message	0
Delete Archive Reply Reply Forward Attachment Move Junk Read/Unread Follow Report Message Coodu of an Расчет заработной платы за текущий месяц • Грачева Алла < AGracheva@ • Гоау at 14:51 • Тоday at 14:51 То: • «.kravcova@ • Тобель учета рабоч… • Сооки • Сооки • Сооки	ало Антифишинг 💿 🛛
 41 КВ Download All Preview All Алиса, добрый день! На настоящий момент у вас насчитывается пропуск двух рабочих дней без уважительной причины. Во вложении и по ссылке доступен табель учета рабочего времени. Необходимо подтвердить информацию о количестве отработаных дней в предыдущем месяце. Если есть бео количестве отработаных дней в предыдущем месяце. Если есть бео количестве отработаных дней в предыдущем месяце. Если есть бео количестве отработаных дней в предыдущем месяце. 	Похоже, вы смогли выявить реальную атаку! Спасибо вам за внимательное отношение к безопасности. Какие эмоции вызвала атака?
Ответ нужно дать до конца рабочего дня, иначе заработная плата за данный месяц будет пересчитана исходя из текущих данных.	Страх × Раздражение Любопытство × Жадность ×
С уважением,	
Главный бухгалтер	Какая это была атака?
Грачева Алла Валентиновна	корпоративная 🗸

Рисунок 19. Выявление реальной фишинговой атаки

Эта функциональность позволяет не только формировать навыки сотрудников, но и побуждать их к безопасному поведению, а также собирать внутренние киберразведывательные (Threat Intelligence) данные по социальной инженерии: техническую и психологическую аналитику по реальным атакам, которые выявили сотрудники.

Использование плагина доступно в Системе, начиная с версии 2.4.3.



9. Результаты учебных атак

В результате каждого действия по каждой имитированной атаке у сотрудника накапливается рейтинг – число, означающее одновременно его опыт и общий уровень защищённости (рис. 20).

ФИО	Электронная почта	Должность	Текущий рейтинг ↑
Donald Peterman	peterman@antph.me	Manager	6 😽 🖉 🔵 выдержал атаку

Рисунок 20. Отображение текущего рейтинга сотрудника

Отрицательный рейтинг означает, что в большинстве имитированных атак сотрудник совершал небезопасные действия (рис. 21).

ΦΝΟ ↓	Электронная почта	Должность	Текущий рейтинг
Cameron Heghi	heghi@antph.me	Manager	-3 -3 🖉 🔵 ввел данные в форму

Рисунок 21. Отображение текущего рейтинга сотрудника

Степень в рейтинге и комментарий означают последние изменения: насколько ухудшилось или улучшилось поведение сотрудника и что именно он сделал в последней имитированной атаке.

Общий рейтинг вкупе с его изменением по всем сотрудникам является ключевым показателем защищённости и отображается на главной странице «Антифишинга» (рис. 22).





Навыки ухудшаются , но у 3 сотрудников рейтинг улучшился

Рисунок 22. Отображение общего рейтинга сотрудников на главной странице

10. Формирование рейтинга

В случае, если сотрудник совершил хоть одно небезопасное действие в атаке, рейтинг в ней автоматически становится отрицательным, так как атака считается не выдержанной.



Соответственно, если сотрудник открыл письмо, но не скачал файл или не перешёл по фишинговой ссылке, то его рейтинг будет равен -1, а «плюсовые» значения по другим действиям уже не будут учтены.

11. История действий

Через «Историю действий» можно посмотреть, как действовал сотрудник (или любая группа коллег) на протяжении времени. Графики наглядно покажут все совершённые операции и изменения рейтинга (рис. 23).



Рисунок 23. Отображение истории действий сотрудников на графиках

Оранжевый график показывает имитированные атаки и статистику, общую для всех выбранных сотрудников.

Синий график показывает статистику по подмножеству выбранных сотрудников (не все выбранные пользователи могли одновременно участвовать в одних и тех же имитированных атаках).



Статистика по обучению и обнаружению уязвимых приложений показана для тех же сотрудников справочно и не влияет на изменение рейтинга.

12. Обучение сотрудников

В Системе есть встроенная система обучения и несколько курсов по вопросам информационной и физической безопасности, которые следует знать сотруднику (рис. 24).

После отправки на обучение (вручную, через планировщик, или через API) пользователю приходит приглашение. Перейдя по ссылке в нём, сотрудник попадает в личный кабинет, где будут отображены все назначенные ему курсы.







Рисунок 24. Раздел обучения

Часть курсов может быть доступной для самостоятельного изучения и будет отображаться без установленного срока прохождения.

Каждый курс состоит из теории и обязательного тестирования.

По большей части материал подаётся в виде жизненных случаев – примеров реальных ситуаций и атак, которые могут встретиться сотруднику, и конкретных практических рекомендаций о том, как действовать в этих ситуациях.





Рисунок 25. Слайд из курса «Безопасная работа в интернете и с электронной почтой»



Рисунок 26. Слайд из курса обучения «Мобильная безопасность»



ООО «МультиТек Инжиниринг»

e-mail: info@mte-cyber.by



Рисунок 27. Слайд из курса обучения «Физическая безопасность»

Примеры слайдов из курсов обучения Системы приведены на рис. 25-27. Вторая часть каждого курса представляет собой обязательный тест (рис. 28), в котором необходимо набрать проходной балл для того, чтобы курс был засчитан как пройденный.





Рисунок 28. Прохождение теста после изучения курса

Все тесты также построены на кейсах — реальных ситуациях, в которых может оказаться сотрудник, и предлагают выбрать правильный вариант действий.

После успешного прохождения обучения каждому сотруднику автоматически выдается сертификат (рис. 29).





Настоящим удостоверяется, что сотрудник:

Иванов Сергей Петрович

прошел обучение и успешно сдал итоговое тестирование по курсу Базовый курс по информационной безопасности

Общий балл за курс: 93 из 100

Балл за тест: 87 из 100

Сертификат действителен до: 31 декабря 2020 года.



Рисунок 29. Сертификат об успешном прохождении курса

Система предоставляет возможность оформлять сертификаты в соответствие с корпоративным брендбуком.

QR-код на сертификате позволяет проверить актуальность действующего сертификата (если сотрудник допустил нарушения, то его могут назначать на повторное обучение, а старые результаты в таком случае станут недействительными).

В Системе доступны следующие учебные курсы:

- Базовый курс по безопасности;
- Безопасная работа в интернете и с почтой;
- Мобильная безопасность;
- Физическая безопасность;
- Безопасная удалённая работа.

Производитель намеренно не создаёт множества курсов – компактно упакованные знания позволяют не перегружать сотрудников, тратить на обучение оптимальное время.



«Антифишинг» может интегрироваться с внешними системами обучения – «ВебТьютор» и Moodle (рис. 30).



Рисунок 30. Схема интеграции «Антифишинга» с внешними системами обучения

При такой интеграции курсы «Антифишинга» поставляются в систему обучения в формате SCORM, сотрудники проходят обучение в привычной им среде, а вся статистика и управление процессом остаются в «Антифишинге».





13. Работа со статистикой и отчётами

Ключевые показатели защищённости всегда доступны на панели мониторинга (рис. 31).

Рисунок 31. Отображение ключевых показателей на панели мониторинга

Расшифровку обозначения каждого сектора можно увидеть при наведении курсора мыши. Статистика по сектору отображается при нажатии на него (рис.32).

Уязвимости

Имеют уязвимые приложения 23% 7 сотрудников имеют уязвимые приложения Назначить обучение

Рисунок 32. Отображение статистики по сектору «Уязвимости»

При нажатии на ссылку информация по соответствующим сотрудникам будет показана в таблице целей. Прямо из панели мониторинга можно выбрать и отправить сотрудников на обучение или проверить их навыки.

Помимо этого, в Системе реализованы возможности по созданию различных отчётов и выгрузке журналов по широкому спектру действий и событий.



e da	•			6				ĸ		M
Антифишинг — Общая статисти	сервис обу ка	мения и контрол	ия защище	нности сотрудни	иков					
218	->	22	÷	18	÷	13	->	6		
COTON/Reaming Salad Africa B CotOrganit		abonation		(The Description of the Control)		nepeuru no counce ana disputa annanasia Asia		иникот укланиция Ириклонения		
9		10		0	->	1	÷	3		
orgende		atax aunonene		сотрудников прошли обучение		на обротник		ходля обучение воерени		
						20				
		-		2. 1	ŕ	15	1	4 4	2 0:	

Рисунок 33. Пример главного отчёта

Главный отчёт (рис. 33) содержит общую статистику:

– общее количество сотрудников, отделов — графики и наглядные представления трендов;

– общее количество сотрудников, которые находятся на обучении, прошли его, не прошли вовремя;

- общее количество проведённых атак с информацией о том, сколько сотрудников прошли атаку и с каким результатом;

- количество выполненных атак;

- количество сотрудников, на устройствах которых имеются уязвимости, перечень брешей и степень их серьёзности.



libri ~ 11 I <u>U</u> ~ ⊞ ~ ≦	~ A` # 2 ~ <u>A</u> ~		Numbe	Conditional F	formatting ~ ble ~	Colls Editing
/ Jx c	D	E	F	G	н	i
Антифицинг — с	POPRAC O	будения и конт	00.00 22	шишенности с	отруды	NKOB
	срвисо	Cynchun u Kont	p07/7 30	цищенности с	отрудн	INOB
Статистика по об	учению	для 70 сотрудн	иков			
По всем курсам		-		_		-
34	\rightarrow	0	\rightarrow	0	\rightarrow	0
не назначалось		прошли обучение		на обучении		не прошли вовреми
Information Const	the Deal					
information Secu	rity Basi	cs		11.047		1941 0020
56	\rightarrow	0	\rightarrow	0	\rightarrow	14
не назначалось		прошли обучение		на обучении		не прошли вовреми
80%		0%		0%	-	20%
Web and Email S	ecurity					
60	\rightarrow	3	\rightarrow	0	\rightarrow	7
		прошан объегине		ua oficiensi		не прошии вовоеми
* 85%		4%		0%	-	10%
Базовый курс по	безопа	сности				
E2	4	2	~	G	2	0
22		2	1	0		9
не назначалось 75%		прошли обучение 2%		на обучении 8%		не прошли вовремя 12%
Базовый курс по	безопа	сности 2020				
60		0		-		
69	\rightarrow	0	\rightarrow	0	\rightarrow	1
не назначалось		прошли обучение		на обучении		не прошли вовреми
98%		0%		0%		15
ьезопасная рабо	та в инт	гернете и с почт	гой			
60	\rightarrow	2	\rightarrow	5	\rightarrow	3
По всем курсам	Попытки	Information Security	y Basics	Web and Email Se	curity	Базовый курс по без

Рисунок 34. Пример отчёта по обучению

Отчёт по обучению (рис. 34) содержит полную статистику по курсам и сотрудникам, которые их проходят:

- статусы по курсу: «прошёл» / «не прошёл» / «отменено»;
- сколько попыток было по каждому курсу;
- детальная отчётность по каждому курсу.



Другие отчёты и журналы действий помогают увидеть всю прочую статистику по процессам в Системе в разных разрезах.

Все журналы и отчёты могут импортироваться в SIEM-систему по протоколу Syslog.

Указанной возможностью пользуются заказчики, которые проводят корреляцию событий из области безопасности, в том числе на основе уровня знаний и поведения сотрудников в имитированных атаках.

Все данные из Системы доступны через АРІ для любых внешних систем, таких, например, как IDM, IRP/SOAR.

Тот же API позволяет управлять процессами из SGRC-решений, таких, например, как R-Vision SGRC.

