



Экосистема **HACKEN**

Август 2017

Белая книга. Версия 001.



Содержание

Содержание

Резюме

В настоящем документе описываются ключевые бизнес-компоненты Экосистемы Hasken. Он также излагает детали продажи токенов Hasken, которая начнется в 00:00 по восточноевропейскому времени 31 октября 2017 года и завершится в 00:00 по восточноевропейскому времени 30 ноября 2017 года. В документе также объясняется последующая дорожная карта создания Экосистемы Hasken, в том случае если продажа токенов достигнет целевых этапов.

Экосистема Hasken — поддерживаемая сообществом торговая площадка в области услуг кибербезопасности, которая станет результатом данной продажи токенов и будет организована в ряде юрисдикций по всему миру. Она состоит из площадки услуг поиска уязвимостей HaskenProof, Платформы вознаграждения за выявление оригинальных уязвимостей нулевого дня, Инкубатора стартапов в области кибербезопасности Hasken, Центра аналитики кибербезопасности и Конференции HaskIT.

Hasken (HKN) — это токен стандарта ERC20, являющийся единственным платежным инструментом допустимым в Экосистеме Hasken. Покупка Hasken сегодня позволит в будущем получать качественные услуги кибербезопасности по привлекательной цене.

Просим принять ко вниманию, что все финансовые данные и юридическая документация, связанные с этой продажей токенов, доступны отдельно от этой белой книги по вашему запросу.

Введение

32 миллиона долларов, украденных у Parity, и 7,4 миллиона у Coindash в 2017 году, 72 у Bitfinex в 2016, 5,1 у Bitstamp в 2015, 65 у Mt. Gox в 2014 году. Эти ужасающие суммы — эквиваленты денег, украденных хакерами в результате взлома различных проектов, обеспечивающих инфраструктуру криптовалют.

Согласно исследованию Тайлера Мура из Факультета компьютерных наук Университета Талсы (Оклахома), с момента создания биткойна в 2009 году по март 2015 года было взломано около 33% всех биткойн-бирж мира. Безусловно, криптовалюты являются далеко не единственной сферой деятельности, испытывающей трудности из-за хакеров. Президент США Дональд Трамп, сам являющийся предметом недавнего хакерского скандала и последовавшего за ним специального расследования, заявил, что киберпреступления являются наиболее быстрорастущим видом преступлений в США. Беспокойство президента подкрепляется реальными деньгами. США инвестируют более 19 млрд. долларов в кибербезопасность в рамках федерального бюджета 2017 года. Эта цифра на 14 млрд. выше аналогичной статьи бюджета на 2016 год, принятого ещё при Бараке Обаме.

К сожалению, на сегодня в мире ещё недостаточно компетентных специалистов, чтобы использовать эти огромные финансовые ресурсы. По данным CyberSeek, в 2017 году более 348 000 вакансий в области кибербезопасности так и не были закрыты, а к 2022 году это число вырастет до 1,8 млн. В сочетании с неучтенным числом «чёрных» хакеров, работающих «по ту сторону файервола», данная статистика требует незамедлительных действий.

До недавнего времени Восточная Европа и, в частности, Украина, были рассадником различных противоречивых онлайн-проектов с сомнительной репутацией. Имея огромное количество высококвалифицированных выпускников физико-математического направления, экономика страны по-прежнему мало что может предложить этим людям. Тем не менее, украинцы являлись основателями таких единорогов Силиконовой долины, как фиатная платёжная система PayPal, программа для обмена мгновенными сообщениями WhatsApp и даже технология WiFi, которую вы, вероятно, используете в данный момент.

Украина также имеет долгую историю довольно непростых взаимоотношений с технологией блокчейн. Несмотря на то, что биткоин

никогда так и не был признан легитимным платёжными инструментом в стране, украинские стартапы и эксперты входят в когорту мировых лидеров блокчейн-революции.

История компании [BitFury](#) является ярким тому подтверждением. BitFury была основана в Киеве в 2011 году. По состоянию на [январь 2017 года](#) эта компания контролировала 9,5% вычислительных мощностей биткоина. Это стало возможным благодаря собственным майнинговым чипсетам, разработанным местными инженерами BitFury.

BitFury также заключила ряд уникальных правительственных контрактов, включая первый в мире проект по обеспечению кадастрового учёта земли при помощи технологии блокчейн, запущенный совместно с правительством Грузии.

Мы считаем, что Украина может стать следующим европейским центром кибербезопасности. Усиление опыта в этой области в настоящее время является вопросом выживания страны, учитывая атаку вируса [Petya.A](#) на инфраструктуру правительственных учреждений, [кибератаку на облэнерго](#) в 2015 году и другие поддерживаемые правительствами соседних государств кибератаки, которые с большой вероятностью ещё неоднократно повторятся. Экспертиза в области блокчейн-технологий также поможет стране, учитывая галопирующую инфляцию гривни в 2014 году, после того как экономика и банковская система пострадали из-за начала военного конфликта.

Тем не менее, появлению этих ярких индустрий кибербезопасности и блокчейна должно способствовать развитое и этичное экспертное сообщество. И оно ведь уже существует, учитывая [лидирующую позицию](#) Украины [в высшей лиге](#) европейского IT-аутсорсинга. Аутсорсинговая экспертиза предоставляет необходимые поступления денег чтобы компьютерные профессионалы чувствовали себя в финансовой безопасности, а некогда мощное физмат образование начало возрождаться. Например, DefConUA — команда этичных хакеров из КПИ им. Игоря Сикорского, стали лучшей CTF-командой 2016 года согласно рейтингу [CTFTime](#).

Наша цель как команды Hacken состоит в том, чтобы заложить структуру сообщества этичных хакеров Восточной Европы, создав стабильные средства дохода и финансовые стимулы для его участников. В конечном счете, ваше участие в Экосистеме Hacken поможет обеспечить то, что следующее поколение местных юных компьютерных дарований будет работать на вашей стороне файервола.

Что такое Экосистема Hacken?

Наша экосистема состоит из токена Hacken, и комплекса предприятий, предоставляющих услуги, которые могут быть получены только с использованием Hacken в качестве платежного инструмента. Количество хакенов конечно, оно ограничено 20 миллионами токенов, подлежащих распределению во время предварительной и основной продажи токенов.

Предприятия, входящие в состав Экосистема Hacken — это площадка услуг поиска уязвимостей HackenProof, Платформа вознаграждения за выявление оригинальных уязвимостей нулевого дня, Бизнес-акселератор в области кибербезопасности Hacken, Центр аналитики кибербезопасности и Конференция HackIT. Каждый элемент нашей экосистемы описывается далее в отдельных разделах этого документа.

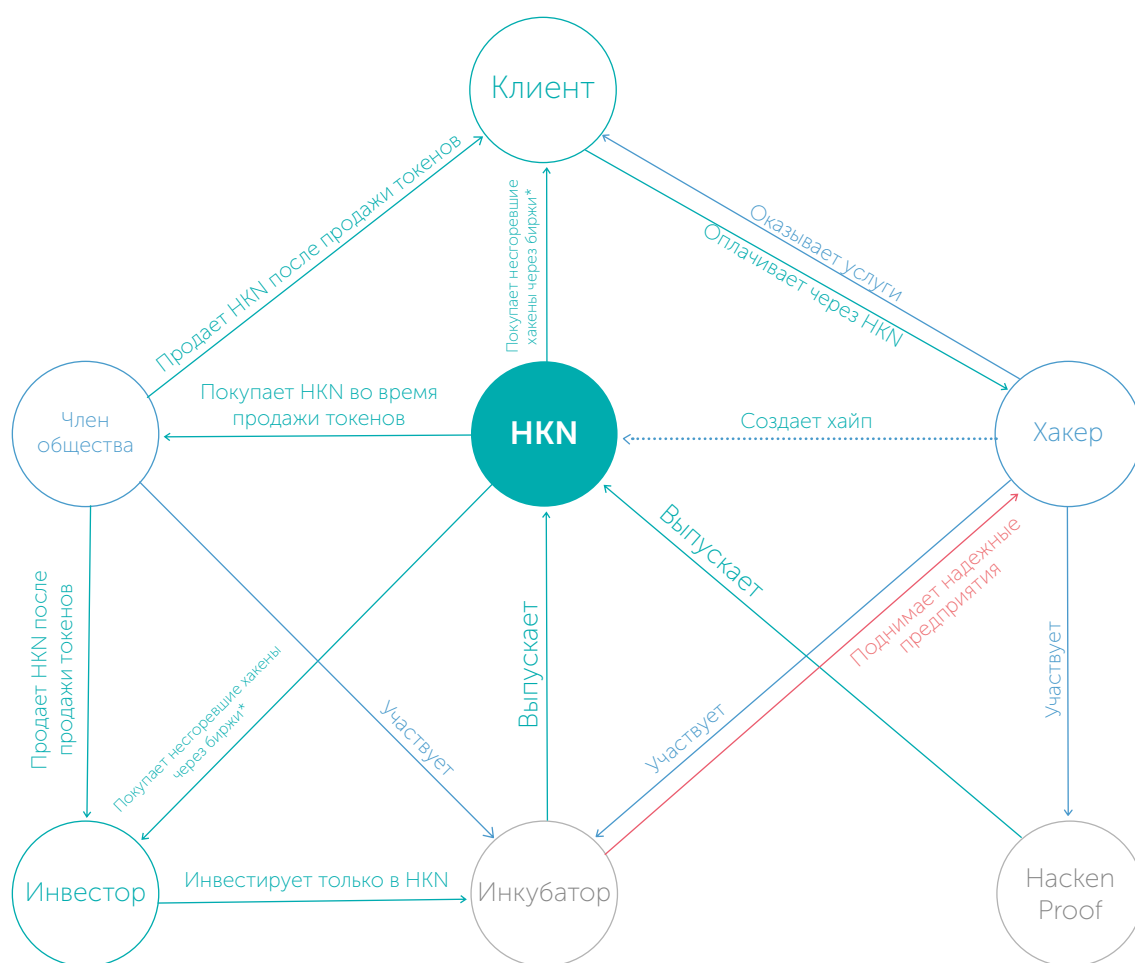


Рис. 1. Экосистема Hacken

Основополагающая идея Nasken заключается в том, что наш токен превращает каждого своего владельца в участника сообщества. Поскольку Nasken является специализированным токеном, в первую очередь ориентированным на профессионалов и проекты в области кибербезопасности, он также объединяет этих людей, создавая стимулы для взаимного ведения бизнеса и инвестиций в стартапы в области кибербезопасности. Участникам сообщества необходимо будет общаться и взаимодействовать друг с другом, чтобы использовать свои хакены. Чем живее сообщество, тем большую ценность оно приносит каждому участнику.

Хотя наша экосистема имеет прочный бизнес-план и дорожную карту продукта, речь идет не только о бизнесе. Нашей целью также является развитие и поддержка разнообразных событий и встреч сообщества в Европе, равно как и в любой другой точке мира, включая NaskIT — крупнейшую в Украине международную конференцию по кибербезопасности. Предприятия в сфере кибербезопасности уделяют очень много внимания экспертным знаниям, этике и постоянному обучению. Поддерживая NaskIT, мы хотим отблагодарить сообщество, расширяющее нашу платформу.

Прекрасной иллюстрацией наших ключевых ценностей является история Алексея Матиясевича — украинского специалиста в области кибербезопасности, архитектора EDCC в Ambisafe и нашего технологического советника в данной продаже токенов.

Этим летом, 19 июля 2017 года, Алексей обнаружил критическую уязвимость в коде кошелька Parity Ethereum. На обсуждения не было времени, поскольку Алексей заметил признаки продолжающейся хакерской атаки, которая впоследствии привела ко взлому сотен кошельков Ethereum. В итоге Алексей перевел эфиры на 1 402 996,09 в долларовом эквиваленте из уязвимых кошельков на те, которые он защитил и контролировал. Затем Алексей связался с группой White Hat Group, взявшей на себя ответственность за поиск и возвращение всех токенов их законным владельцам.

Конечной целью нашей экосистемы является создание поколения хакеров, для которых то, что сделал Алексей, является вполне нормальным, единственным приемлемым сценарием жизни.

Как Hacken использует блокчейн?

Доказательство тестирования уязвимостей

После подписания клиентом соглашения об участии в кампании поиска уязвимостей, наша команда создает соответствующий блокчейн-блок, содержащий данные о продукте, условия соглашения об обслуживании и отметку времени. Следующий блок цепочки, индивидуальный для каждого клиента, будет содержать информацию об уязвимостях, обнаруженных во время наших исследований безопасности.

После того как клиенты устраняют уязвимости, обнаруженные во время нашей кампании по их поиску, эксперты HackenProof проводят пост-исследовательский аудит. Затем мы обсуждаем наши выводы с клиентами и сообщаем о всех дополнительных мерах, которые необходимо принять. Если результаты аудита являются удовлетворительными для обеих сторон — нашей команды и команды клиентов — мы формируем следующий блок в цепочке, содержащий информацию об устранённых проблемах.

В конце концов, клиенты получают Сертификат уязвимостей и контрмер HackenProof, содержащий отчет обо всех обнаруженных и устраненных уязвимостях с отметкой времени для каждого события. Затем клиенты могут настроить предпочтения публичности сертификата и сделать изложенную в нём информацию доступной широкой общественности, клиентам, инвесторам или тем, кого они назначат.

Криптовалюта

Помимо использования блокчейна в кибербезопасности, эта продажа токенов также имеет интересную финансовую инновацию в области криптовалют. Это наш принцип «сгорания», который мы объясняем [в отдельном разделе](#) этого документа.

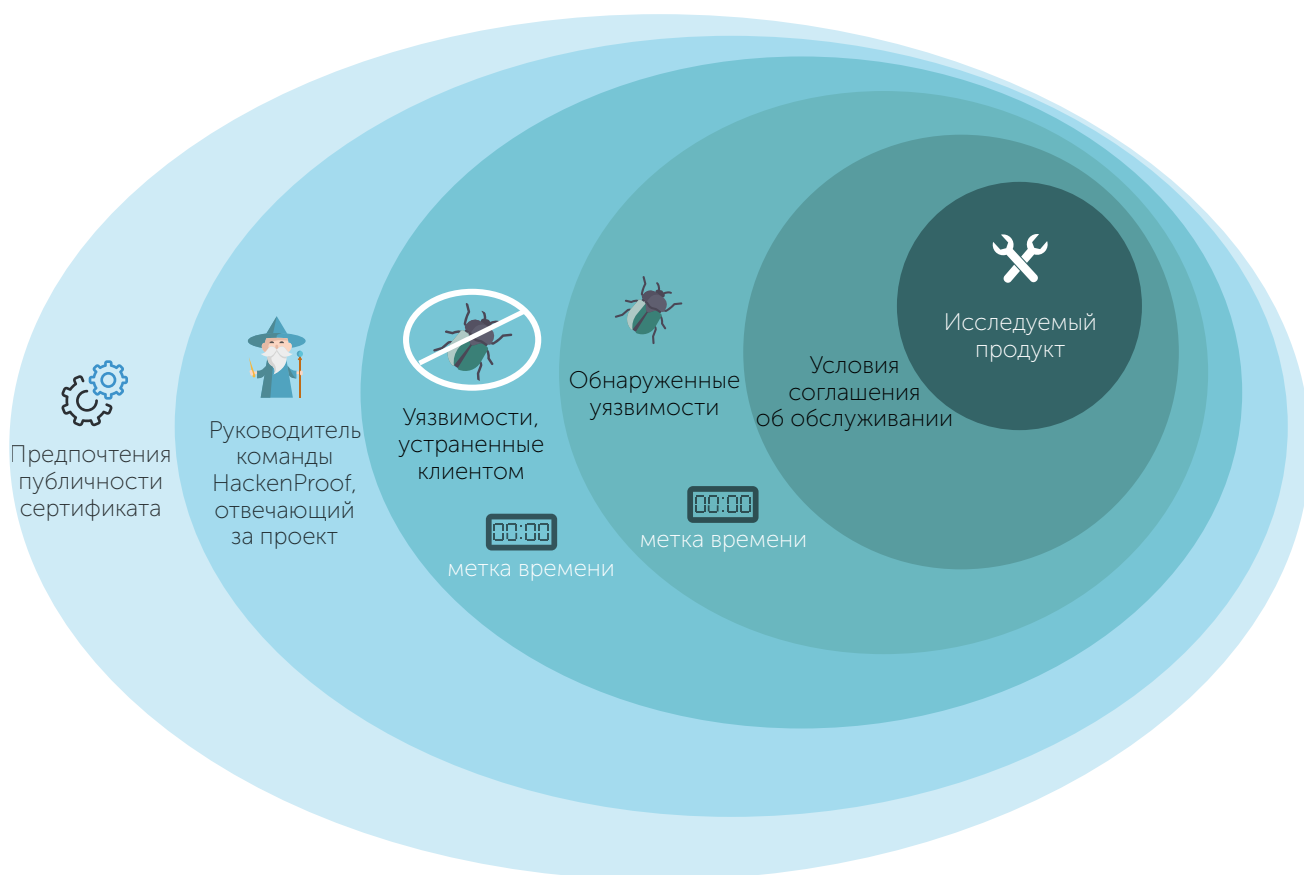


Рис. 2. Сертификат уязвимостей и контрмер HackenProof

Зачем нужна ещё одна площадка для услуг поиска уязвимостей?

Как вы можете видеть из [краткого анализа рынка](#) в Приложении к настоящему документу или из ваших собственных наблюдений, уже существует, по крайней мере, четыре действующих площадки поиска уязвимостей и тестирования проникновения. Каждая из них имеет растущую клиентскую базу и финансовую поддержку инвесторов в диапазоне от нескольких до 74 млн. долларов США. Напрашивается очевидный вопрос: действительно ли на рынке поиска уязвимостей нужна еще одна площадка?

Мы думаем, что да. И вот почему:

- 1 / В настоящее время спрос в области тестирования проникновения и программ поиска уязвимостей превышает предложение.

Недавно Mazda спонсировала конкурс CTF в Лас-Вегасе, в котором победитель получил грузовик. После взлома Jeep, Tesla и Nissan LEAF автомобильная промышленность отчаянно нуждается в высококвалифицированных исследователях уязвимостей и тестирующих проникновения. В нашей ситуации это означает: нет, четырех существующих площадок совершенно недостаточно. На рынке по-прежнему существует голубой океан нишевых и общеспециализированных услуг кибербезопасности.

- 2 / **Наша экосистема кибербезопасности специально разработана для технологии блокчейн.** Будучи блокчейн-предпринимателями, мы понимаем эту технологию, её нюансы, риски и сообщество лучше, чем большая часть нынешнего истеблишмента кибербезопасности. Читать о блокчейне в Wall Street Journal, обсуждать его с коллегами за чашкой кофе и инвестировать несколько тысяч долларов в биткойн только ради удовольствия — это одно. Основывать весь свой бизнес, денежные потоки предприятия и технологии сертификации услуг на блокчейне — совсем другая история.
- 3 / **Забыли ли мы об МСП?** Малые и средние предприятия не могут позволить себе преимущества тестирования проникновения и программ поиска уязвимостей. Это не значит, что они им не нужны. В нынешней среде кибербезопасности иметь малый бизнес означает иметь очень ограниченный доступ к преимуществам современной инфраструктуры компьютерной безопасности. Мы предоставим МСП простые и удобные онлайн-инструменты для организации и проведения кампаний по поиску ошибок и тестированию проникновения.
- 4 / **Общий часовой пояс и культурные ценности.** Наскен будет одним из первых движителей на европейском рынке в сфере поиска уязвимостей. В настоящее время на этом рынке доминируют предприятия, базирующиеся в Силиконовой долине. Это совершенно понятно, но Сан-Франциско и Область залива — не единственное место в мире, где создаются хорошие программные и аппаратные проекты. По-прежнему существует достаточный спрос на услуги от команд, базирующихся в других частях мира и обеспечивающих хорошее соотношение цены и качества.

Токен Hacken

На протяжении тысячелетий деньги были эффективным, но не основным фактором в объединении человеческих организаций, а также в стимулировании их последующего роста и развития. Hacken — не исключение. Распределенный характер блокчейна позволяет нам быстро создать новый токен и наполнять его лучшими качествами современной валюты. Технология интеллектуальных контрактов позволяет добавить дополнительное смысловое измерение в Hacken и создать экономические стимулы для сообщества кибербезопасности, чтобы объединиться и сотрудничать на этических и законных основаниях.

Hacken — единственная валюта, допустимая внутри нашей экосистемы. Любые новые заказы через HackenProof, Платформу вознаграждения за выявление оригинальных уязвимостей нулевого дня, Центр аналитики кибербезопасности либо новые инвестиции через бизнес-акселератор Hacken должны осуществляться в хакенах. Такой подход будет вознаграждать участников сообщества, получающих оплату в хакенах, обеспечивая положительную ликвидность и низкую волатильность.

Обратите внимание: хакены не предназначены быть электронными деньгами, товаром для продажи или любым другим финансовым инструментом, не представляют собой акции, доли, обеспечения либо эквивалентных прав, включая, помимо прочего, любое право на получение будущего дохода и прав интеллектуальной собственности. Хакены также не являются объектом права собственности.

Продажа HKN

Помимо использования блокчейна в кибербезопасности, в процессе подготовки к продаже токенов наша команда осуществила ряд финансовых инноваций в сфере криптовалюты. Это и есть наш принцип «сгорания», который мы описываем в отдельном разделе данного документа.

Общее количество	20 млн. хакенов 1,3 млн. — предварительная продажа (1 млн. + 30% бонус) 18,7 млн. — основная продажа токенов	
Символ	HKN	
Минимальная сумма к продаже	1 ETH	
Максимальный предел	20 млн. Никаких будущих эмиссий не планируется	
Первоначальный эквивалент стоимости	1 HKN = 1 USD	
Принимаемые валюты	BTC, ETH, DASH, LTC, USD, EUR, TaaS	
Продолжительность продажи токенов	31 октября 2017 года — 30 ноября 2017 года	
Эскроу	в среднем 80% собранных средств хранится на целевом депозитном счете	
* Бонусная программа для основной продажи токенов	1 — 4 часа	25%
	1 — 2 дня	20%
	3 — 7 дней	15%
	1 — 2 недели	10%

Рис. 3. Детали продажи токенов

Распределение токенов

Открытая продажа	80%
Вознаграждение команды	10%
Вознаграждение советников	7%
Вознаграждение Менеджера сообщества	1%
Премия за продажу токенов, из которой:	2%
Сообщения в блогах	0.8%
BitcoinTalk Signature	0.3%
Перевод BitcoinTalk	0.3%
BitcoinTalk Thread	0.2%
Твиты	0.2%
Посты в Фейсбуке	0.2%

Рис. 4. Цепочка распределения токенов

Основные вехи

Обязательство	«Минимальная» веха	«Ограниченная» веха	«Целевая» веха	«Продвинутая» веха	«Максимальная» веха
Количество проданных токенов	1.5 млн.	4 млн.	10 млн.	16 млн.	20 млн.
Конференция HackIT	15%	10%	10%	5%	5%
Площадка HackenProof	85%	75%	65%	40%	40%
Аналитический центр	—	15%	15%	10%	10%
Платформа нулевого дня	—	—	15%	35%	30%
Акселератор Hacken	—	—	—	10%	15%

Рис. 5. Основные вехи

Дорожная карта

Проект/ Распределение ресурсов	2017 4-й кв.	2018 1-й кв.	2018 2-й кв.	2018 3-й кв.	2018 4-й кв.	2019	2020
Конференция HackIT	—	—	—	50%	—	33%	32%
Площадка HackenProof	10%	20%	10%	10%	10%	25%	15%
Бизнес-акселератор Hacken	5%	5%	10%	10%	15%	30%	25%
Платформа нулевого дня	5%	5%	10%	15%	15%	25%	25%
Аналитический центр	2.5%	5%	5%	7.5%	7.5%	37.5%	35%

Рис. 6. Дорожная карта

Периоды запуска:

Площадка HackenProof – 4-й кв. 2017 г.

Аналитический центр – 1-й кв. 2018 г.

Бизнес-акселератор Hacken – 4-й кв. 2017 г.

Платформа нулевого дня – 3-й кв. 2018 г.

Конференция HackIT – 3-й кв. 2018 г., новые конкурсы и выступления на HackIT 2018 будут поддерживаться Hacken.

Принцип «сгорания»

Мы изобрели принцип «сгорания» для этой продажи токенов чтобы устранить регуляторные риски, которые в противном случае могли бы препятствовать участию клиентов, являющихся резидентами некоторых юрисдикций. Мы также считаем, что «сгорание» ускорит рост ликвидности и уменьшит риски волатильности для HKN. Всем владельцам хакенов важно понять, что «сгорание» влияет только на суммы, входящие в комиссию платформы. Таким образом уменьшается количество хакенов, которыми владеем мы, основатели платформы, а не наши клиенты.

Что происходит с остальными 50% нашей маржи на обслуживании, которые не сгорают? Управляющая компания Экосистемы Hacken будет накапливать эти хакены, пока их количество не достигнет 1% от общего количества хакенов в обращении.

После наступления этого события мы сделаем объявление за 24 часа, а затем продадим 1% от суммы, накопленной на момент события (то есть 0,01% от общей суммы хакенов, находящихся в обращении на момент события) через основные биржи криптовалют. Продажа каждый раз будет происходить в 14:00 по восточноевропейскому времени на следующий день после объявления. Список бирж будет предоставлен общественности во время первой подобной продажи. Мы оставляем за собой право вносить изменения в список бирж в будущем.

«Сгорание» изменяет установленный обменный курс хаков к другим фиатным валютам и криптовалютам. Это необходимо, чтобы сохранить достойные ценовые показатели за услуги по поиску уязвимостей, привлечь больше хакеров на платформу HackenProof, а также обеспечить стабильное и эффективное обслуживание нашей экосистемы. Все данные о «сгорании» будут прозрачны и доступны для общественности через наш вебсайт.

Проект	Принцип «сгорания»	Уведомление	Время
HackenProof	50% от маржи обслуживания платформы для каждой транзакции. В настоящее время оценочная средняя маржа за услуги HackenProof составляет 30% на транзакцию, а это означает, что 15% от каждой транзакции, связанной с услугами HackenProof, будут «сгорать».	За 24 часа до сгорания	Ежедневно в 12:00 дня по восточно-европейскому времени
Бизнес-акселератор Hacken	50% от маржи акселератора во время «выхода» стартапа. По очевидным причинам трудно точно оценить точную маржу при выходе. Мы ожидаем, что инвестиционные репликаторы будут находиться в диапазоне 10 и выше.		
Платформа нулевого дня	50% годовой прибыли, полученной управляющей компанией Hacken с обеих операций. Сумма прибыли будет рассчитываться на основе финансовой отчетности, проверенной авторитетным международным аудитором.	За одну календарную неделю до осуществления «сгорания»	Ежегодно после аудита финансовой отчетности
Аналитический центр			

Рис. 7. Принцип «сгорания»

Эскроу и аудит

Эскроу-агенты вовлечены в процесс хранения и управления активами инвесторов. Их функция заключается в мониторинге использования собранных средств в соответствии с дорожной картой, описанной в данном документе. Эскроу-агенты могут наложить вето на транзакцию, применив криптографический ключ к кошельку нашего проекта, используемому для накопления средств инвесторов.

Поставщиками целевого депозитного счета будут Juscutum и одна из аудиторских компаний Большой четверки, выбранная путём тендера, организованного Общественным советом попечителей Экосистемы Hacken. Juscutum является украинской юридической фирмой, расположенной в Киеве, и оказывает юридическую поддержку предприятиям блокчейн-экосистемы. Для HackenProof и Конференции HackIT 70% привлеченных средств будет храниться на эскроу-депозите. Целевой депозитный счет будет открыт для 100% бюджетных расходов на разработку и развитие Платформы нулевого дня, бизнес-акселератора Hacken и Аналитического центра кибербезопасности.

Ежегодный аудит финансовой отчетности юридических лиц, входящих в Экосистему Hacken будет проводиться международно-признанной аудиторской компанией, отобранной посредством тендера, управляемого Общественным советом попечителей Экосистемы Hacken.

Отказ от ответственности

Этот документ, а также любая другая документация и информация, предоставленные вместе с ним, не являются офертой либо предложением купить или продать акции или ценные бумаги. Ничто из представленных сведений не предназначено стать частью и не должно считаться основанием для какого-либо инвестиционного решения.

Экосистема Hacken не предоставляет консультаций по инвестициям, адвокатской помощи или ходатайства об инвестировании в какую-либо ценную бумагу, и её деятельность не должна толковаться таким образом.

Этот документ не входит, не является частью и не должен рассматриваться как какое-либо предложение о продаже или подписке, или какое-либо приглашение покупать или подписываться на какие-либо ценные бумаги или другие финансовые инструменты.

HackenProof

HackenProof — это платформа рынка поиска уязвимостей, созданная этичными хакерами и блокчейн-сообществом на основе принципа справедливого участия. Это место, где оба сообщества могут сотрудничать и поддерживать друг друга. Целями данного сотрудничества является высококачественное тестирование проникновения и отчеты об уязвимости за премиальную оплату, выплачиваемую членам сообщества, представляющим эти отчеты.

Как это работает?

- 1 / Клиенты подписываются на программу поиска уязвимостей, выбирают определенную политику программы, принимают решения о приглашениях и вознаграждениях и устанавливают уровень выплаты бонусов.
- 2 / Наши специалисты помогают клиентам установить и настроить свою программу, а также управлять ею, если это будет необходимо.
- 3 / По установлении рамок оценки безопасности наша команда приглашает участников сообщества Hacken принять участие в оценке. Сотни белых хакеров оценивают код клиента на предмет уязвимостей и ошибок.
- 4 / Члены сообщества представляют уязвимости и определяют их приоритетность. Их отчеты проверяются на актуальность и оригинальность.
- 5 / Члены сообщества получают плату за обнаружение ценных уязвимостей.
- 6 / Клиент может дополнительно заказать у команды архитекторов решений безопасности Hacken советы по разработке контрмер, если это необходимо.
- 7 / Клиент получает сертификат об уязвимостях, подтверждающий, что его программное обеспечение было изучено и проверено сообществом Hacken. По желанию в сертификате может быть отдельный раздел «Контрмеры», в котором будут перечислены все проблемы, обнаруженные и исправленные клиентом.

Гарантия возврата денег

Через некоторое время после запуска мы реализуем функционал гарантии возврата денег. За дополнительную плату клиент сможет приобрести наши услуги с этой опцией.

Таким образом, если после завершения изучения уязвимостей и выдачи Сертификата уязвимостей и контрмер HackenProof, клиент обнаружит не указанную в этом сертификате существенную уязвимость, клиент может потребовать возврата вознаграждения за наши услуги. Экспертиза указанной уязвимости на предмет её «существенности» будет проводиться третьей стороной, определяемой положениями контракта между клиентом и HackenProof.

Ключевые особенности

Скрытое или публичное приглашение — уровень общественной видимости вашей программы поиска уязвимостей может быть настроен в зависимости от ваших целей.

Самостоятельное или выделенное управление — ваша программа может быть настроена в зависимости от вашего бюджета и уровня знаний.

Портал самообслуживания клиентов с широким диапазоном гибкости. Вы можете запустить мастер для определения и запуска вашей программы, бот будет проверять отчеты и устранять дубликаты. Затем вы можете настроить выплаты, чтобы предлагать бонусы за самые ценные открытия.

Настраиваемая и герметичная среда тестирования, предоставляемая решениями VDI, VPN и PAM позволит участвующим в кампании исследователям лучше понимать инфраструктуру клиента, не причиняя никакого вреда или беспокойства.

Платформа вознаграждения за выявление оригинальных уязвимостей нулевого дня

Мы создадим фонд вознаграждения за выявление оригинальных уязвимостей нулевого дня. Hacker будет поддерживать ярких и этичных экспертов в области компьютерных технологий, финансово вознаграждая их за оригинальные и ранее нераскрытые исследования уязвимостей нулевого дня.

Мы понимаем юридические и этические риски данного мероприятия, но наше видение заключается в том, что исследования уязвимостей нулевого дня должны иметь прозрачный и публичный канал вознаграждения. В противном случае они окажутся не в тех руках. В настоящее время основным риском данной отрасли является то, что многие элементы исследований нулевого дня по собственной инициативе исследователя считаются незаконными во многих юрисдикциях. Такая позиция некоторых государств замедляет развитие исследований подобных уязвимостей, а также проверенных каналов вознаграждения за их исследование.

Регулярные несоответствия приводят к риску уголовного преследования этических экспертов, открыто проводящих свои исследования на благо человечества, в то время как «черные» хакеры обычно избегают любого наказания, выполняя «грязную работу» для частных картелей или правительств стран-изгоев. Причиной этого является отсутствие эффективных механизмов расследований Интернет-преступлений высокой сложности и несовершенство процедуры сбора доказательств местными правоохранительными органами. В случае же финансируемого государством незаконного вмешательства в работу компьютерных систем, мы имеем дело не с противодействием, а с прямой государственной поддержкой.

Мы установим этические и анонимные бизнес-процессы для талантливых специалистов, исследующих подобные уязвимости. Мы планируем инвестировать значительный объем средств, привлеченных во время этой продажи токенов, в исследование соответствующей нормативно-правовой базы в ключевых юрисдикциях, в частности — в Европе. Конечной целью является создание прозрачной нормативной базы для нашей Платформы нулевого дня до начала её деятельности.

Мы хотели бы установить специальные скидки для членов нашего сообщества по подписке на нашу Платформу нулевого дня. Тем не менее, важно, чтобы члены сообщества Hacken понимали, что по этическим и регуляторным причинам их участие в этой продаже токенов автоматически не предоставляет им доступ к Платформе.

Общественный совет попечителей Платформы нулевого дня разработает правила доступа и проведет процесс отбора. Этот совет будет создан в течение одного года после продажи токенов, если мы достигнем рубежа, позволяющего начать работу над созданием Платформы нулевого дня. Подробнее смотрите раздел **«Основные вехи»** выше. Совет будет состоять из самых уважаемых и опытных членов нашего сообщества.

Бизнес-акселератор Hacken

Прекрасно, когда ваши сотрудники решают начать свой бизнес. Это показатель того, что нынешняя работа развивает, вдохновляет и расширяет их возможности.

В 2000-х годах Google начал стимулировать сотрудников к «совместительству» и разработке собственных проектов и продуктов. В конечном итоге это привело к появлению Google Ventures, одного из самых уважаемых и инновационных венчурных фондов в мире.

Мы сами являемся владельцами предприятий в области кибербезопасности и поэтому видим огромную открытость и потенциал восточноевропейского рынка кибербезопасности. Честно говоря, сейчас ему требуются более качественные игроки и более инновационные бизнес-модели.

Самая большая текущая проблема заключается в отсутствии навыков привлечения надежных инвесторов и создания прозрачной корпоративной структуры среди восточноевропейцев, решивших начать собственное дело в области кибербезопасности. Это приводит к довольно ограниченному количеству заметных сделок в данной отрасли в нашей части мира. Отсутствие крупных игроков стало причиной малого количества бизнес-ангелов, готовых поддержать стартапы, находящиеся на ранней стадии развития. Вследствие этого ошибки и возникающие в результате неудач травмируют молодых основателей, отталкивая их от самой идеи начать свой собственный бизнес.

Мы считаем, что Hacken может разбить этот порочный круг, создав солидную репутацию среди инвесторов и владельцев бизнеса, а затем поручившись за лучших и наиболее ответственных участников нашего сообщества. К тому времени будем знать, кем они являются, руководствуясь не только их презентациями и профилями в LinkedIn, но и их проектами в реальной жизни и последствиями повседневного стресса, возникающего у любого предпринимателя вследствие жёсткого контроля рубежных сроков и бизнес-показателей.

Выбрав этих начинающих предпринимателей, мы «прокачаем» их знания. Слушая наших лучших клиентов и членов сообщества, которые уже управляют собственным бизнесом, они будут вдохновляться и вырастать, готовясь стать следующим поколением лидеров в области кибербезопасности.

Польза для инвесторов

- 1 / Мы софинансируем проекты и разделяем риски с инвесторами. Nasken будет инвестировать до 25% стоимости стартапов, которые мы будем акселерировать.
- 2 / Маркетинговая платформа Nasken и наша маркетинговая команда будут готовы обучать участников акселератора совместно разрабатывать стратегию выхода на рынок и помогать им успешно её выполнять.
- 3 / Аналитический центр Nasken поможет участникам акселерационной программы изучать конкуренцию и соответствующие клиентские сегменты, а также разрабатывать уникальное торговое предложение для клиентов.

Аналитический центр кибербезопасности

Мы собираемся создать группу аналитиков, проводящих фундаментальные исследования в области кибербезопасности, а также занимающихся мониторингом и аудитом существующих и будущих продуктов в области кибербезопасности.

Затем наша команда начнёт представлять корпоративные исследования в области кибербезопасности, экспертизу и независимые исследования, а также сравнение этих продуктов.

Основной информационный бюллетень Центра будет находиться в открытом доступе через веб-сайт Hacken и социальные сети. Вся углубленная аналитика будет доступна на основе платной подписки и почтового приобретения.

Области исследований

- Безопасность блокчейна, уязвимости и контрмеры;
- Классификация, сравнение и исследование рынка продуктов кибербезопасности;
- Криптография, защищенная связь и защита данных;
- Аналитика крупных массивов данных и визуализация в кибербезопасности.

Команда

Центр возглавит хорошо известная команда-победитель различных конкурсов CTF и её международные советники. Основной задачей команды будет разработка инфраструктуры и рамочных решений для исследования и анализа 30 и более различных видов продуктов кибербезопасности.

Мы также планируем организовать постоянную стажировку в Центре для студентов из Украины и из-за рубежа. Самым вероятным источником талантов станут финалисты и победители Конференции HackIT.

Конференция HackIT

HackIT — это ежегодный международный форум по кибербезопасности, проходящий в Харькове, Украина. Первая Конференция HackIT собрала 450 участников из двух стран, вторая — 650 участников из шести стран. Помимо традиционных дискуссий с участием местных и международных экспертов, HackIT проводит ряд специализированных соревнований по кибербезопасности, участие в которых бесплатно для всех желающих.

Конкурс CTF

Конкурс HackIT Capture the Flag (CTF) состоится 25—27 августа этого года. Хакеры будут соревноваться в 8 категориях: Web, Misc, Joy, Crypto, PWN, Reverse, Forensics и Stego.

В 2016 году мероприятие собрало более 5000 уникальных онлайн-участников из 1062 команд из 93 стран. Победитель мероприятия — команда DCUA из Украины, позже стала лучшей командой мира 2016 года в соответствии с рейтингом CTF Time.

«Битва хакеров»

Отборочный тур на это соревнование проходит в первой половине конференции, а финал — во второй половине. Во время отборочного тура каждый участник должен за 30 минут решить максимальное количество задач по кибербезопасности и заработать очки. Финалисты, заработавшие максимальные баллы, затем выходят на подиум для решения проблемы кибербезопасности в режиме реального времени. Их компьютерные экраны транслируются для зрителей, и их работа освещается в прямой трансляции в стиле киберспорта.

Кубок HackIT

Этот конкурс собирает 30 самых ярких хакеров со всего мира, которые стали победителями HackIT CTF. Участники укрепляют свои навыки и создают еще более сильное сообщество. Им также будет предоставлена возможность участвовать в частной программе поиска уязвимостей с мгновенной оплатой.

В этом году отчеты об уязвимостях будут представлены клиентам на борту Ан-225 «Мрия» — самого большого самолета в мире.

Конференция HackIT. Быстрые факты

- 1 / HackIT — это мероприятие, проводимое сообществом и одобренное местными группами OWASP и DEF CON.
- 2 / На конференции были представлены доклады отраслевых лидеров, включая CheckPoint, EY, Samsung, Cyphort и GlobalLogic.
- 3 / Помимо конференции HackIT, предлагается три онлайн-конкурса: CTF, Битва хакеров и Вызов кибердетектива OSINT.
- 4 / В HackIT CTF 2016 приняли участие более 5000 участников из 93 стран.
- 5 / Победитель HackIT CTF 2016 — команда DCUA стала лучшей командой CTF 2016 года согласно рейтингу CTFtime.org.



КТО МЫ?

Большую часть своей карьеры были вовлечены в различные проекты в отрасли кибербезопасности. Мы давно рассматриваем Украину как страну огромного потенциала в области кибербезопасности. Недавние кибератаки на инфраструктуру страны, в которых заметен след нашего соседа, заставили нас поверить, что наше время наступило.

Дмитрий является сертифицированным международным бухгалтером и аудитором. Он работал в Deloitte в течение 8 лет на различных должностях по бухгалтерскому учету, аудиту и управлению проектами. В настоящее время он является одним из топ-менеджеров оборонной промышленности Украины после того, как правительством в 2014—2015 годах была начата масштабная реформа. В Deloitte Дмитрий стал победителем «Конкурса Делойт Аудит СНГ» со своим решением SAP Bid Data, которое широко внедрялось в различных офисах Deloitte в СНГ и существенно повысило эффективность проектов Deloitte.



Дмитрий Будорин

финансовый директор
и ведущий менеджер
Hacken



Никита Кныш

директор по связям
с сообществом

Никита специализируется в области обучения кибербезопасности различных государственных учреждений Украины. Он является генеральным директором ProtectMaster, одной из наиболее авторитетных фирм по кибербезопасности Украины. Никита — советник по кибербезопасности Администрации Президента Украины и соучредитель конференции HackIT.

У Андрея за плечами 13 лет успешной карьеры в области кибербезопасности. Он работал на корпоративных клиентов, интеграторов и успешно управлял сложными техническими решениями в нескольких странах для корпораций, правительственных учреждений, банков и даже Международного олимпийского комитета. Он является сертифицированным специалистом по ряду технологий, включая таких поставщиков, как CheckPoint, Cisco и Juniper Networks. Его роль в проекте заключается в технологическом лидерстве разработки, интеграции и поддержки платформы HackenProof.



Андрей Матюхин

технический директор



Д-р Егор Аушев

исполнительный директор

Егор получил степень доктора наук в области физики высоких энергий в DESY, Гамбург. Он является автором 22 научных работ в этой области. С 2015 года Егор является генеральным директором Information Security Group — нишевой фирмы в области кибербезопасности, предоставляющей услуги по тестированию проникновения, защите данных и аудиту информационной безопасности.

Почему это имеет значение?

Не новость, что кибербезопасность в настоящее время — такая же горячая тема, как и криптовалюты. Также неудивительно, что Восточная Европа сейчас стала испытательным полигоном для кибервойны.

Украина является печально известной иллюстрацией того, как традиционные учреждения не смогли защитить тех, для кого они были созданы. Частичным оправданием здесь является наш нереформированный постсоветский менталитет, который не был готов к экспоненциальным цифровым угрозам мира, уже ставшего «плоским».

Технология блокчейн также находится под ударом и в настоящее время также стала полигоном для различных техник проникновения и взлома, как мы уже определили во вступительном разделе выше. Количество вариантов применения блокчейна растёт с каждым днём, привлекая всё большее внимание хакеров.

В то же время в эти последние бурные годы мы наблюдали феномен, совершенно новый для нашей части мира, а именно — гражданский киберактивизм. В случае Украины, обычные люди: университетские профессора, бизнес-консультанты, адвокаты и банковские работники объединили свои усилия по созданию коллективной системы кибербезопасности страны. Мы уже видели аналогичную ситуацию три года назад во время военного конфликта в Украине, происходившего в реальном пространстве.

Этот активизм не только дает веру и надежду, но также является основой возникновения успешных бизнес-моделей. В конце концов, западные файерволы также не выдержали в 2015—2017 годах, несмотря на лучшую институциональную культуру, хорошо зарекомендовавшую себя систему обучения и, самое главное, бюджеты в области обороны, которые нельзя даже сравнить с восточноевропейскими.

Криптовалюты играют жизненно важную роль в создании значительных, распределенных и прозрачных бюджетов киберзащиты, созданных при помощи прямой поддержки частных лиц. Они позволяют обходить традиционную институциональную сеть, которая в этом случае позволяет достичь цели только тогда, когда уже слишком поздно.

Эта продажа токенов, если она будет успешной, позволит нам не только создать прочную региональную систему кибербезопасности, но и адаптироваться к вызовам, которые, несомненно, появятся в течение следующего десятилетия. Это могло бы также инициировать движение, которое через несколько лет станет важным фактором сдерживания и противодействия международной киберпреступности, в том числе и финансируемой отдельными государствами.

Наш эксперимент в Hacked начинается с очевидной бизнес-модели: площадки для поиска уязвимостей и краудсорсинговой платформы тестирования проникновения. Хотя некоторые подобные платформы уже существуют, мы считаем, что под солнцем по-прежнему много места, как мы объясняли в отдельном разделе этого документа.

Затем мы планируем развернуть экосистему в двух своих самых рискованных направлениях: Фонд уязвимостей нулевого дня для покупки критических уязвимостей на сером рынке и бизнес-акселератор для стартапов в области кибербезопасности и блокчейн-технологий. Да, в настоящее время появилось слишком много стартапов со словами «кибер» и «блокчейн» в названии. Но в данном случае подумайте не о бизнес-оппортунисте, а о местном самообразованном инженерере с ограниченным владением английским языком (на данный момент), но с головой, полной ярких идей. Подумайте о человеке, который может создать новый WiFi или BitFury. Мы знаем, что подобные люди существуют на нашей опушке леса. Мы знаем наставников, которые помогут им развить свои идеи до коммерческого уровня и создать следующее поколение продуктов в области безопасности технологии блокчейн.

Фонд нулевого дня, возможно, сначала покажется не связанным с бизнес-акселератором, но это не так. Чтобы отвлечь умных

восточных европейцев от сомнительных источников дохода, мы сначала предложим узаконить их работу, приобретая уязвимости, которые они обнаруживают, и удостоверяться в том, что подобные уязвимости раскрываются легитимным сторонам, прежде всего — поставщикам данных технологий. Затем мы предложим жизнеспособную альтернативу взлому, который в свою очередь со временем будет становиться все более автоматизированным и рутинным. Альтернатива, которую мы продвигаем, — это запуск легитимного бизнеса и прекращение зависимости от дона, платящего за мелкую грязную работу.

Наконец, отбирая лучшие таланты из существующей экосистемы, мы хотим убедиться, что возвращаем ей должное. Эти усилия — наша поддержка Конференции HackIT и создание Аналитического центра кибербезопасности.

HackIT уже служит региональной витриной для нашей профессии. Он является вдохновением для будущих поколений и местом обмена знаниями между состоявшимися и стремящимися к этому профессионалами в области кибербезопасности. Затем Аналитический центр будет поддерживать тех людей, которые не хотят начинать свой бизнес и более склонны к академической и исследовательской карьере, продвигая фундаментальную науку кибербезопасности.

Есть еще много проектов на будущее, и они уже находятся в нашей дорожной карте и на нашем радаре. Однако мы понимаем, что существующие этапы уже и так довольно амбициозны и потребуют нашей полной самоотдачи, по крайней мере, в течение нескольких лет. Поэтому сейчас нам лучше делать то, что должно быть сделано в первую очередь, а затем — «поживем-увидим», как говорится в известной пословице.


Мы надеемся, что этот документ привел твердые аргументы, подробную информацию и в конечном итоге убедил вас принять участие в продаже хакенов. Если это так — добро пожаловать в Экосистему Hacken, и вскоре вы станете уважаемым членом сообщества либо нашим клиентом. Если нет, мы будем рады предоставить вам дополнительную помощь и более подробную информацию по info@hacken.io или через наш твиттер [Hacken_io](https://twitter.com/Hacken_io).

Приложение.

Краткий анализ существующего бизнеса по краудсорсингу исследований уязвимостей

Функция	Bugrowd	HackerOne	Synack	Cobalt	HackenProof
Страна	США	США / Нидерланды	США	США	Эстония / Украина
Сегмент рынка	Массовый	Массовый	Корпоративный	Корпоративный	Гибридный
Программа тестирования проникновения	Нет	Нет	Да	Да	Да
Модель подписки	Нет	Нет	Да	Да	Да
Консалтинг ¹	Да	Да	Да	Да	Да
Частный поиск уязвимостей	Да	Да	Нет	Нет	Да
Список ведущих исследователей ²	Да	Да	Нет	Нет	Да
Разработка программных бюллетеней по ошибкам ³	Да	Да	Нет	Нет	Да
Управляемая платформа ⁴	Да	Да	Нет	Нет	Да
Поиск уязвимостей по времени (по запросу) ⁵	Да	Да	Нет	Нет	Да
Общедоступный поиск уязвимостей	Да	Да	Нет	Нет	Да
Возвращение денег	Нет	Нет	Нет	Нет	Да
Расширенные функции	Собственная VPN-технология ⁶	Автоматическое удаление дубликатов	Гидра-сканнер ⁷	Не определено	а. Умный портал ⁸ б. Мастер настройки для бонусной программы с. Автоматическое устранение дубликатов

Рис. 9. Существующие предприятия по краудсорсингу исследования уязвимости

- 
- ¹ Функции тесного контакта, в том числе возможность иметь экспертную информацию об уязвимостях, которые могут быть сильно эксплуатироваться.
 - ² Исследователям разрешен доступ к частным программам поиска ошибок.
 - ³ Помимо хостинга платформы для управления программой клиента.
 - ⁴ В средах с ограниченными ресурсами клиент может захотеть передать часть своей программы на аутсорсинг.
 - ⁵ Эти типы бонусных программ, как правило, имеют меньшую продолжительность и ограниченные расходы, а это означает, что вы можете ограничить свои расходы, связанные с рамочным контентом и тем самым конкурировать с традиционными аутсорсинговыми тестированиями проникновения.
 - ⁶ Позволяет исследователям просматривать конкретный контент программы через свой портал.
 - ⁷ Расширенная платформа интеллектуального анализа уязвимостей для автоматизации рутинных процессов.
 - ⁸ Виртуальная инфраструктура рабочего стола для кампании по поиску уязвимостей на месте. Виртуальная частная сеть для кампании по поиску уязвимостей на месте. Предпочтительное решение для безопасности учетной записи для кампании по поиску уязвимостей на месте.

Список рисунков и таблиц