Аннотация – в документе представлен анализ "Europol Cybercrime Training Competency Framework 2024", направленного на расширение возможностей академических, правоохранительных, криминалистических х и учреждений в борьбе с киберпреступностью. Рассматриваются различные критические аспекты системы, включая определение основных наборов навыков для ключевых участников, участвующих в противодействии киберпреступности, процесс разработки системы и её стратегический контекст в рамках более широкой стратегии ЕС по борьбе с организованной преступностью на 2021–2025 годы.

Документ служит ценным ресурсом для понимания подходов к подготовке сотрудников правоохранительных и судебных органов к киберпреступности и реагирования на них и наращивания потенциала в борьбе с киберпреступностью, способствуя тем самым безопасности и устойчивости цифровых пространств по всему ЕС и за его пределами.

I. Введение

Документ "Europol Cybercrime Training Competency Framework 2024" охватывает широкий спектр материалов и, связанных с обучением по борьбе с киберпреступностью, рамками компетенций, стратегиями и законодательством. Эти материалы (как подборка от Европола) в совокупности направлены на расширение возможностей, судебных и правоохранительных органов и других заинтересованных сторон в эффективной борьбе с киберпреступностью.

Ключевые аспекты включают подход и сферу охвата программы детализации функциональных компетенций, необходимых правоохранительным органам и судебной системе, а также гибкость и адаптируемость программы к различным организационным структурам, а также конкретные роли, обозначенные в рамках концепции, такие как, среди прочего, руководители подразделений по борьбе с киберпреступностью, руководители групп, криминалисты и специализированные эксперты по борьбе с киберпреступностью.

- **Система компетенций Европола по обучению борьбе с киберпреступностью:** описывает наборы навыков, необходимых для различных должностей в правоохранительных и судебных органах для эффективной борьбы с киберпреступностью. Подчёркивается важность цифровой криминалистики, расследований сетевых инцидентов, программирования и специальных знаний о киберпреступности среди других навыков.
- **Инициативы Европейского союза**: Документы подчёркивают усилия ЕС по укреплению возможностей борьбы с киберпреступностью с помощью EC3 (Европейского центра по борьбе с киберпреступностью) и сотрудничества с такими организациями, как CEPOL и ECTEG в части обучения, оперативной поддержки и разработки согласованной правовой базы для борьбы с киберпреступностью.
- **Глобальные и национальные стратегии**: В различных источниках обсуждаются глобальные и национальные стратегии в области законодательства о киберпреступности и наращивания потенциала. ITU Toolkit по законодательству о киберпреступности и руководство Интерпола по национальной стратегии борьбы с киберпреступностью содержат руководящие принципы для разработки эффективных законов и стратегий в области киберпреступности. В этих стратегиях подчёркивается необходимость гармонизации законов, наращивания потенциала органов уголовного правосудия и международного сотрудничества.
- **Обучение**: Важность подготовки при расследовании киберпреступлений подчёркивается в нескольких источниках. Национальный учебный центр по борьбе с киберпреступностью (CyTrain) и орган по расследованию киберпреступлений (CIBOK) предлагают специализированное обучение для сотрудников правоохранительных органов и других заинтересованных сторон. Эти учебные программы охватывают различные аспекты расследования киберпреступлений, включая цифровую криминалистику, анализ разведданных и управление.
- **Сотрудничество и обмен информацией**: Необходимость сотрудничества между правоохранительными органами, частным сектором, научными кругами и международными организациями является постоянной темой. Эффективная борьба с киберпреступностью требует междисциплинарного подхода, обмена передовым опытом и использования экспертных знаний из различных секторов.
- **Законодательство и правовые рамки**: отмечаются проблемы и рекомендации по обновлению правовых рамок для эффективной криминализации

киберпреступлений и судебного преследования за них. Подчёркивается необходимость принятия законов, идущих в ногу с технологическими достижениями и способствующих международному сотрудничеству.

- **Наращивание потенциала и распределение ресурсов**: подчёркивается необходимость наращивания потенциала правоохранительных и судебных органов посредством обучения, предоставления технических ресурсов и создания специализированных подразделений для рассмотрения дел о киберпреступлениях. Это включает в себя устранение пробелов в навыках, знаниях и технологиях

II. Фреймворк

- **Цель**: направленность на определение необходимых наборов навыков для ключевых участников, участвующих в борьбе с киберпреступностью. Является руководством для правоохранительных органов, судебных органов и академических учреждений по пониманию компетенций, необходимых для эффективного противодействия растущей угрозе киберпреступности.
- **Процесс разработки**: Структура была разработана после процесса консультаций с участием многих заинтересованных сторон. Сюда вошли материалы различных европейских органов, таких как Агентство Европейского союза по подготовке сотрудников правоохранительных органов (CEPOL), Европейская группа по обучению и просвещению в области киберпреступности (ECTEG), Евроюст, Европейская судебная сеть по борьбе с киберпреступностью (EJCN) и представители, назначенные Целевой группой Европейского союза по борьбе с киберпреступностью (EUCTF).
- **Стратегический контекст**: обновлённая структура является частью плана действий Европейской комиссии, направленного на укрепление потенциала правоохранительных органов в цифровых расследованиях. Это согласуется со Стратегией ЕС по борьбе с организованной преступностью на период 2021–2025 годов.
- **Сфера применения и ограничения**: Система фокусируется на уникальных навыках, имеющих отношение к расследованиям киберпреступлений и работе с цифровыми доказательствами. Она не охватывает все навыки, необходимые для выполнения описанных ролей, но подчёркивает те, которые характерны для киберпреступности. Структура не является исчерпывающим перечнем навыков или одобрением структуры конкретного подразделения или профилей сотрудников. Он предназначен для наращивания стратегического потенциала в организационных структурах правоохранительных органов и судебной системы.
- **Гибкость и адаптация**: В зависимости от организационной структуры и штатного расписания роли и соответствующие наборы навыков, изложенные в структуре, могут быть объединены или переданы на аутсорсинг специализированным подразделениям, таким как уголовный анализ и криминалистика.
- **Функциональные компетенции**: Структура определяет основные функциональные компетенции, необходимые правоохранительным органам для эффективной борьбы с киберпреступностью. Особое внимание уделяется конкретным навыкам, необходимым для расследования киберпреступлений и обращения с цифровыми доказательствами, а не общим навыкам правоохранительных органов.
- **Неполный список навыков**: не предоставляется исчерпывающего списка навыков, но фокусируется на тех, которые имеют уникальное отношение к расследованиям киберпреступлений. Такой подход позволяет целенаправленно развивать компетенции, наиболее важные в контексте киберпреступности.
- **Наращивание стратегического потенциала**: предназначение в качестве инструмента для наращивания стратегического потенциала в правоохранительных и судебных учреждениях направленность на повышение компетентности, имеющей решающее значение для эффективного рассмотрения дел о киберпреступлениях.
- **Исключение общих навыков**: Общая подготовка сотрудников правоохранительных органов, управленческие навыки и "софт склиз" не включены в рамки, что гарантирует, что фреймворк ориентирован на специализированные навыки, необходимые для противодействия преступности
- **Процесс разработки**: фреймворк разработан с помощью комплексного процесса, который включал онлайн-анкеты, очный семинар и анализ ответов заинтересованных сторон. Такой совместный подход обеспечил отражение текущих потребностей и будущих требований правоохранительных органов и академических учреждений.
- **Матрица компетенций**: Матрица компетенций является центральным элементом структуры, описывающей необходимые роли, наборы навыков и желаемые уровни квалификации для практикующих специалистов. Эта матрица служит наглядным руководством для понимания конкретных компетенций, необходимых для выполнения различных функций в рамках расследований киберпреступлений.
- **Описания ролей**: Подробные описания основных функций и наборов навыков для различных ролей

представлены по всему документу. Эти роли включают, среди прочего, руководителей подразделений по борьбе с киберпреступностью, руководителей групп, криминалистов, аналитиков по киберпреступности и специализированных экспертов. Каждая роль адаптирована для решения конкретных аспектов киберпреступности и обработки цифровых доказательств.

- **Наборы навыков и уровни**: Структура описывает конкретные наборы навыков, необходимые для каждой роли, и желаемые уровни мастерства. Эти наборы навыков включают, среди прочего, цифровую криминалистику, сетевые расследования, программирование и законодательство о киберпреступности. Подчёркивается важность наличия спецнавыков, которые непосредственно применимы к проблемам киберпреступности.

III. Роли

- **Руководители подразделений по борьбе с киберпреступностью**: отвечают за надзор за подразделениями по борьбе с киберпреступностью, принятие обоснованных решений по случаям киберпреступности, координацию ресурсов и расстановку приоритетов в деятельности полиции. Они должны иметь всестороннее представление о возможностях подразделения и обеспечивать необходимое обучение и инструменты для персонала. Навыки эффективного общения и управления взаимоотношениями, особенно на английском языке, необходимы для взаимодействия с международными заинтересованными сторонами.
- **Руководители групп**: руководят расследованиями киберпреступлений в своих конкретных областях. Они контролируют текущие расследования, координируют работу со старшим руководством и обеспечивают, чтобы их команда была оснащена необходимой подготовкой и инструментами. Как и руководителям подразделений, им требуется практический опыт оценки оперативной деятельности и сильные коммуникативные навыки.
- **Криминалисты**: чаще сталкиваются с кибер-элементами в различных преступлениях. Им необходимо фундаментальное понимание цифрового мира, в том числе того, как обращаться с электронными доказательствами на местах преступлений и эффективно использовать разведданные из открытых источников (OSINT).
- **Аналитики по киберпреступности**: Аналитики участвуют в сборе и анализе данных для получения оперативной информации и стратегических выводов. Им необходимо обрабатывать большие объёмы данных из различных источников и преобразовывать их в краткие отчёты. Обмен информацией с более широкой аудиторией и участие в стратегических совещаниях также являются частью их роли.
- **Криминалисты по киберпреступности**: глубоко разбирающиеся в извлечении данных и онлайн-сборе информации, и руководят расследованиями киберпреступлений и часто участвуют в обучении других инструкторов из числа сотрудников правоохранительных органов.
- **Эксперты по киберпреступности**: обладают специализированными знаниями в конкретных областях киберпреступности, таких как OSINT, дарквеб, криптовалюты и устройства Интернета вещей. Оказывают оперативную поддержку в расследованиях и должны постоянно совершенствовать свои навыки посредством обмена опытом между коллегами на национальном и международном уровнях.
- **Цифровые криминалисты**: сосредоточены на выявлении, восстановлении и анализе цифровых доказательств. Они знакомы с различными операционными системами, инструментами судебной экспертизы и обладают навыками написания сценариев и программирования. Они также готовят доказательства для сложных задач дешифрования и сообщают о своих выводах.
- **Эксперты по реагированию на кибератаки**: Эти эксперты отвечают за техническое реагирование на кибератаки, сотрудничая с различными заинтересованными сторонами, такими как группы реагирования на компьютерные аварийные ситуации (CERT) и ИТ-отделы. Они несут ответственность за сохранение цифровых доказательств и обеспечение их целостности для судебных процессов.
- **Специалисты первой инстанции**: являются сотрудниками правоохранительных органов, первыми прибывающими на место кибер-инцидента. Им необходимы базовые знания в области цифровой криминалистики и киберпреступности, а в их обязанности входит идентификация и обеспечение сохранности электронных доказательств в соответствии с национальными правилами и передовой практикой.
- **Судьи первой и апелляционной инстанций**: судьям, рассматривающим дела о киберпреступлениях, необходимо эффективно интегрировать кибер-доказательства в судебный процесс. Они должны поддерживать знания о киберпреступности и цифровых доказательствах.
- **Прокуроры и судьи-следователи**: Эти юристы руководят уголовными расследованиями, связанными с кибернетическими элементами, оценивают сбор электронных доказательств и представляют дела в суде. Им требуется базовое понимание цифрового мира и способность использовать разведданные из различных источников, включая OSINT, в дополнение к своим расследованиям

IV. Навыки

- **Цифровая криминалистика**: включает идентификацию, сохранение, приобретение, валидацию, анализ, интерпретацию, документирование и представление электронных доказательств из цифровых источников. Ключевые области включают криминалистику данных в реальном времени, облачную, мобильную, сетевую криминалистику, криминалистику ОС, файловой системы, Интернета вещей, и криптографию.
- **Исследование и администрирование сети**: относится к пониманию сетевых функций, проведению расследований внутри сетей и анализу данных о трафике для выявления признаков компрометации. Навыки включают сетевое администрирование, оперативный сбор сетевых данных, сетевую криминалистику и анализ данных о трафике, а также опыт в расследованиях киберпреступлений и хранении доказательств.
- **Программирование и написание сценариев**: используется для построения информационных систем и автоматизации задач для поддержки исследований и анализа данных. Языки программирования включают, среди прочих, Python, JavaScript, Java и C ++. Навыки охватывают разработку бэкенда, фронтэнда и full-стек.
- **Составление отчётов и представление данных расследований киберпреступлений**: включает документацию, составление заметок и составление окончательного отчёта по различным типам отчётов. В нем подчёркивается важность структурированной отчётности, которая является фактической, заслуживающей доверия и приемлемой в суде. Навыки презентации включают синтез информации и адаптацию сложных технических тем для нетехнической аудитории.
- **Анализ и визуализация**: включает применение методов анализа данных для описания, иллюстрации и обобщения данных о киберпреступлениях с целью выявления закономерностей, тенденций и практических знаний. Навыки требуют опыта в области сбора данных, разработки исследований, статистических методов, визуализации передового опыта и этических соображений при обработке данных о преступлениях.
- **Законодательство о киберпреступности**: относится к пониманию законодательства, регулирующего киберпреступную деятельность, включая национальное законодательство о киберпреступности и электронных доказательствах, законы о конфиденциальности, Общие положения о защите данных (GDPR), правила ЕС о хранении данных и решения международных судов.
- **Общие знания о киберпреступности**: охватывает информацию, касающуюся киберпреступлений с поддержкой киберпространства и кибер-зависимости, тенденций киберпреступности, угроз и методов работы, а также понимание кибербезопасности.
- **Специальные знания о киберпреступности**: относятся к уникальным навыкам, полученным в результате специальной подготовки в конкретных областях киберпреступности. Области включают OSINT, даркверб, блокчейны и криптовалюты, анализ вторжений и реагирование на инциденты, этичный взлом, анализ угроз, а также анализ вредоносных программ и обратный инжиниринг.
- **Управление на месте преступления и обработка электронных доказательств**: относится к стандартам и передовой практике выявления и изъятия электронных доказательств на местах преступлений. Навыки включают сбор, упаковку, передачу и хранение устройств, которые могут содержать электронные доказательства, а также проведение опросов на месте происшествия и оказание поддержки жертвам.
- **Методы расследования киберпреступлений**: включает навыки, необходимые для расследования киберпреступлений, такие как методы сбора разведданных, обработка и интерпретация данных, отслеживание подозреваемых онлайн и офлайн, работа под прикрытием онлайн, допрос киберпреступников и управление рисками расследования