DOI: 10.18137/RNU.V9187.23.04.P.116 УДК 004.056

А.Р. Кузьмин, М.Ф. Савельев

ПРИМЕНЕНИЕ МОДЕЛИ ОБЪЕДИНЕННОЙ ЦЕПОЧКИ ВРАЖДЕБНЫХ ДЕЙСТВИЙ (THE UNIFIED KILL CHAIN) ДЛЯ КОММЕРЧЕСКИХ БЕСПИЛОТНЫХ АВИАЦИОННЫХ СИСТЕМ

Аннотация. Целью статьи является анализ применимости модели объединенной цепочки враждебных действий (The Unified Kill Chain) для беспилотных авиационных систем, преимуществ обеспечения информационной безопасности беспилотных авиационных систем от применения данной модели. В настоящей работе авторы использовали метод системного анализа открытых источников по теме, а также синтез на его базе. Результатом применения данных методов стали описанные применительно к беспилотным авиационным системам этапы the Unified Kill Chain и выработка подходов к минимизации актуальных угроз безопасности беспилотных авиационных систем. Представленная статья является одной из первых работ, посвященных применению the Unified Kill Chain в интересах информационной безопасности беспилотных авиационных систем.

Ключевые слова: беспилотные авиационные системы, беспилотные летательные аппараты, информационная безопасность, модель объединенной цепочки враждебных действий, the Unified Kill Chain.

A.R. Kuzmin, M.F. Saveliev

APPLICATION OF THE UNIFIED KILL CHAIN MODEL FOR COMMERCIAL UNMANNED AIRCRAFT SYSTEMS

Abstract. The purpose of the article is to analyze the applicability of The Unified Kill Chain model for unmanned aircraft systems, the benefits for ensuring the information security of unmanned aerial systems due to the use of this model. In this work, the authors use the method of system analysis of open sources on the topic, as well as synthesis based on it. The application of these methods resulted in the stages of The Unified Kill Chain model described in relation to unmanned aerial systems and the development of approaches to minimizing actual threats to the safety of unmanned aerial systems. The presented article is one of the first works devoted to the use of The Unified Kill Chain for UAS' information security.

Keywords: unmanned aerial systems, unmanned aerial vehicles, Information Security, The Unified Kill Chain.

Введение

В настоящее время использование беспилотных летательных аппаратов (далее – БПЛА) в гражданских целях становится всё более распространенным. Однако вместе с возможностями, которые предоставляют БПЛА, появляются и новые угрозы безопасности. Для защиты гражданских беспилотных авиационных систем, которые состоят из БПЛА, наземной станции управления и линии связи, необходимо применять соответствующие методы и технологии, основанные на анализе угроз и сценариев их реализации [1]. Один из таких методов – ***модель объединенной цепочки враждебных действий*** (англ. – The Unified Kill Chain, UKC), разработанная для обеспечения безопасности военно-промышленного комплекса, но которая может применяться и для гражданских систем. В данной статье рассматривается, как применение метода UKC может помочь обеспечить безопасность гражданских беспилотных авиационных систем (далее – БАС), а также какие преимущества эта модель может предоставить для совершенствования системы безопасности воздушного транспорта. Кроме того, рассматривается пример построения UKC

Кузьмин Александр Ростиславович
аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ», Санкт-Петербург. Сфера научных интересов: информационная безопасность киберфизических систем, распределенные реестры, разведка по открытым источникам. Автор пяти опубликованных научных работ. ORCID: 0000-0002-0393-412X.
Электронный адрес: alexander.kouzmin@gmail.com

Савельев Максим Феликсович
кандидат технических наук, доцент кафедры информационной безопасности, Санкт-Петербургский электротехнический университет «ЛЭТИ», Санкт-Петербург. Сфера научных интересов: искусственный интеллект, информационная безопасность, беспилотный транспорт. Автор более 10 опубликованных научных работ.
Электронный адрес: mfsavelev@etu.ru

для БАС. Модель является результатом гибридного научно-исследовательского подхода, который объединил этапы UKC и тактик MITRE ATT&CK, как указано в Таблице 1.

Таблица 1

Сравнение моделей*

№	Этапы	Модели		
		Cyber Kill Chain®	**MITRE ATT&CK™**	**The Unified Kill Chain**
1	Reconnaissance (Разведка)	+	+	+
2	Resource Development (Освоение ресурсов)	+	+	+
3	Delivery (Доставка)	+	+	+
4	Social Engineering (Социальная инженерия)	–	–	+
5	Exploitation (Эксплуатация)	+	–	–
6	Persistence (Натиск)	+	+	–
7	Defense Evasion (Преодоление защиты)	–	+	+
8	Command & Control (Получение управления и контроля)	+	+	+
9	Pivoting (Перехват инициативы)	–	–	+
10	Discovery (Осмотр)	–	+	+
11	Privilege Escalation (Эскалация привилегий)	–	+	+
12	Execution (Исполнение вредоносного кода)	–	+	+
13	Credential Access (Доступ к учетным данным)	–	+	–
14	Lateral Movement (Свобода действий)	–	+	–
15	Collection (Сбор защищенных данных)	–	+	+
16	Exfiltration (Эксфильтрация)	–	+	+
17	Impact (Воздействие)	–	+	+
18	Objectives (Цели)	+	–	+

**Источник: здесь и далее таблицы составлены авторами.*

Как мы видим из Таблицы 1, UKC включает в себя 7 этапов, MITRE ATT & CK – 14 этапов, UKC совмещает всё и охватывает 18 тактик атак, которые можно использовать для описания фаз современных кибератак.

Злоумышленники обычно объединяют отдельные этапы UKC для достижения промежуточных целей в поэтапном продвижении к достижению целей конечных: внутренние, промежуточные и внешние. Чтобы получить доступ к этим системам или данным, злоумышленник может использовать первые (внутренние) этапы UKC (этапы 1–8, см. Таблицу 1), чтобы прорваться за периметр организации и проникнуть внутрь. Как только злоумышленник попадает в целевую сеть, могут потребоваться дополнительные привилегии для получения доступа к активам, которые позволяют злоумышленнику выполнять действия над целями атаки (промежуточные этапы 9–14, см. Таблицу 1). Попадая в целевую сеть и взламывая сеть по мере необходимости, злоумышленник может получить привилегии, необходимые для выполнения действий, направленных на цели атаки (внешние этапы 15–18, см. Таблицу 1).

Основное предположение UKC, которое опровергает UKC, заключается в том, что злоумышленник «должен успешно пройти через каждый этап цепочки, прежде чем он сможет достичь желаемого». В отдельных атаках некоторые тактики могут проявляться не в ожидаемой последовательности или вообще игнорироваться. Основываясь на этом первоначальном предположении, защитники могут, естественно, сосредоточить свои усилия на предотвращении кибератак на самых ранних этапах. Тот факт, что фазы атаки могут быть пропущены, существенно влияет на стратегии защиты. Это, в частности, включает в себя создание, защиту и мониторинг областей меньшего обхвата, которые вынуждают злоумышленников начинать заново, прежде чем они смогут действовать для достижения своих целей. Эти области могут быть созданы с помощью таких мер, как сегментация сети в сочетании с изоляцией зон управления идентификацией и доступом. Таким образом, организации потенциально могут значительно повысить свою устойчивость, сосредоточив свои усилия на фазах атак, происходящих в пределах их внутренней сети, которые прокладывают путь к достижению целей.

UKC состоит из следующих этапов, как это показано на Рисунке 1:

• Reconnaissance (Разведка) – исследование, идентификация и выбор целей с использованием активной или пассивной разведки;

• Resource Development (Освоение ресурсов) – подготовительные мероприятия, направленные на создание инфраструктуры, необходимые для атаки;

• Delivery (Доставка) – методы, приводящие к доставке оружия жертве;

• Social Engineering (Социальная инженерия) – приемы, направленные на манипулирование людьми для совершения небезопасных действий;

• Exploitation (Эксплуатация) – методы использования уязвимостей в системах, которые могут привести к выполнению кода;

• Persistence (Сохраняемость) – любой доступ, действие или изменение в системе, которые обеспечивают постоянное присутствие злоумышленника в системе;

• Defense Evasion (Уклонение от защиты) – методы, которые злоумышленник может специально использовать для уклонения от обнаружения или обхода средств защиты;

• Command & Control (Командование и контроль) – методы, которые позволяют злоумышленнику взаимодействовать с контролируемыми системами в целевой сети.

• Pivoting (Поворот) – туннелирование трафика через контролируемые системы в другие системы, к которым нет прямого доступа;

• Discovery (Обнаружение) – методы, которые позволяют злоумышленнику получить информацию о системе и ее сетевой среде;

• Privilege Escalation (Повышение привилегий) – результат методов, которые предоставляют злоумышленнику более высокие разрешения в системе или сети;

• Execution (Исполнение) – методы, которые приводят к выполнению контролируемого злоумышленником кода в локальной или удаленной системе;

• Credential Access (Доступ к учетным данным) – методы, приводящие к доступу или контролю над учетными данными системы, службы или домена;

• Lateral Movement (Горизонтальное перемещение) – методы, позволяющие злоумышленнику получить горизонтальный доступ к другим удаленным системам и управлять ими;

• Collection (Сбор) – методы, используемые для идентификации и сбора данных из целевой сети перед эксфильтрацией;

• Exfiltration (Эксфильтрация) – методы, которые помогают злоумышленнику удалить данные из целевой сети;

• Impact (Воздействие) – методы, направленные на манипулирование, прерывание или уничтожение целевой системы или данных;

• Objectives (Цели) – социально-технические задачи атаки, направленные на достижение стратегической цели.

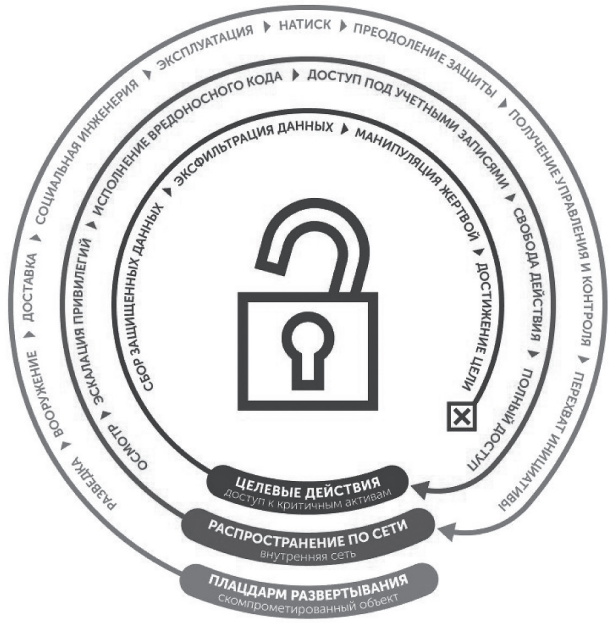

Рисунок 1. Этапы UKC
Источник: [2].

Таким образом, применение модели UKC может помочь обеспечить безопасность гражданских БАС путем улучшения процесса анализа и классификации угроз, а также путем выбора и реализации наиболее эффективных мер безопасности.

В тематических исследованиях [3; 4] длина цепочки, характерной для конкретной атаки, зависит от количества различных тактик, которые атакующий использует для дости-

жения своей цели. Следовательно, продолжительность цепочек, связанных с конкретной атакой, в значительной степени определяется оборонительной позицией организаций-мишеней. Чем сильнее система безопасности, тем длиннее, как ожидается, будет цепочка враждебных действий.

Обеспечение безопасности гражданских БАС

Концепция модели UKC представляет собой методологию для анализа кибератак, которая позволяет описывать типичные этапы атаки – от исходного взлома до целевых действий злоумышленника. Эта методология может быть применена для оценки и обеспечения безопасности различных систем, в том числе гражданских БАС.

Применение UKC в контексте гражданских БАС может улучшить их безопасность, предотвратить утечку конфиденциальной информации, а также защитить от возможных атак на системы управления и автоматизации. Например, на первой стадии взлома может быть использован фишинг, при котором злоумышленник получает доступ к учетной записи пользователя и далее может распространять вредоносные программы на другие устройства и системы. Определение этапов атаки позволяет принимать меры для защиты от уязвимостей на каждом этапе и обеспечить более эффективную систему защиты.

Для гражданских БАС важно проводить анализ уязвимостей, а также тестирование на проникновение, чтобы выявить возможные угрозы и недостатки в системах управления и защиты. В целом применение модели UKC может помочь повысить безопасность гражданских БПЛА и уменьшить вероятность успешных кибератак.

Применение модели UKC обеспечит безопасность гражданских БПЛА, позволив компаниям, производящим их, эффективно анализировать и классифицировать потенциальные угрозы безопасности. С помощью этого метода можно стандартизировать и упорядочить различные фазы, которые могут быть использованы хакерами для атаки на систему БАС, – от фазы разведки до фазы эксплуатации.

Кроме того, использование модели UKC позволит компаниям разработать более эффективные стратегии защиты от атак на стадии планирования и эскизного проектирования, оценить потенциальные уязвимости в подсистемах БАС и разработать меры защиты и контрмеры, чтобы предотвратить возможные атаки.

Таким образом, применение модели UKC может значительно улучшить безопасность гражданских БАС, обеспечив производителям более эффективное и систематическое понимание потенциальных угроз безопасности и соответствующие меры противодействия.

Преимущества для совершенствования системы безопасности воздушного транспорта

Модель UKC может предоставить несколько преимуществ для совершенствования системы безопасности воздушного транспорта.

1. Усиленный мониторинг и обнаружение потенциальных угроз безопасности. Применение модели UKC позволяет оперативно отслеживать не только конечную точку атаки, но и все ее этапы. Это повышает шансы обнаружения угроз безопасности на ранних стадиях их развития и позволяет принимать меры для предотвращения атаки.

2. Анализ и улучшение существующей системы безопасности. Применение модели UKC позволяет проводить детальный анализ происходящих угроз и выявлять слабые места в существующей системе безопасности. На основе полученной информации можно принимать меры для устранения уязвимостей и улучшения существующей системы безопасности воздушного транспорта.

3. Обучение и повышение квалификации персонала. Применение модели UKC позволяет создавать единую методологию обучения и повышения квалификации персонала по вопросам безопасности, что помогает повысить уровень осведомленности и компетентности сотрудников в области информационной безопасности.

UKC для БПЛА

Создание собственной UKC для гражданских БАС поможет в реализации эффективной стратегии защиты и снижении риска уязвимостей. Из рассмотренных ранее примеров можно составить схему, представленную в Таблице 2 [5–7].

Таблица 2

Пример модели UKC беспилотной авиационной системы

№ п/п	Фаза атаки	Пример атаки
1	Reconnaissance (Разведка)	Определение уязвимостей системы безопасности, физической безопасности и сетевой инфраструктуры. Может содержать следующие шаги: исследование технических характеристик и процесса проектирования БПЛА, БАС в целом. Анализ потенциальных уязвимостей системы безопасности, физической безопасности и сетевой инфраструктуры, проведение пен-теста (процесса тестирования на проникновение) на БАС, чтобы определить уязвимости системы безопасности и проверить ее защиту от атак; оценка физической безопасности БАС: проверка механизмов блокировки и защиты от несанкционированного доступа к самим устройствам, съемным устройствам хранения данных, портам коммуникаций и др.; анализ сетевой инфраструктуры БПЛА; проверка наличия защищенного соединения с устройством; проверка защищенности паролей; проверка наличия защиты от внешних атак на соединения. Кроме того, данная фаза может начинаться со сбора общедоступной, открытой информации об объекте атаки с помощью методов разведки по открытым источникам
2	Resource Development (Освоение ресурсов)	Получение необходимых средств и ресурсов для проведения атаки, например захвата управления БПЛА. Может содержать следующие шаги: исследование модели и производителя БПЛА, его технических характеристик и характеристик сетевой инфраструктуры, которая используется для управления БПЛА; анализ протоколов управления БПЛА и поиск уязвимостей в этих протоколах; идентификация возможных точек входа в сеть управления БПЛА, таких как точки доступа Wi-Fi или другие устройства, которые могут использоваться для связи с БПЛА; получение доступа к сети управления БПЛА за счет использования уязвимости в протоколах управления или другие методы, такие как перехват трафика или взлом пароля
3	Delivery (Доставка)	Осуществление доставки вредоносного программного обеспечения или других атакующих средств, а также проведение физической атаки, например, атакующий может использовать различные методы, такие как радиочастотный блокировщик, чтобы вынудить БПЛА перейти в режим возврата на домашнюю базу или сбросить его на землю
4	Social Engineering (Социальная инженерия)	Использование социальных методов, таких как фишинговые атаки, для получения доступа к системе управления БПЛА или к другим уязвимостям
5	Exploitation (Эксплуатация)	Использование уязвимостей для получения доступа к системе управления БПЛА или другим системам, которые могут быть использованы для атаки

Продолжение таблицы 2

№ п/п	Фаза атаки	Пример атаки
6	Persistence (Натиск)	Маскировка следов атаки и обеспечение долговременного доступа к управлению БПЛА. Некоторые из методов включают в себя использование криптографии и шифрования для скрытия передачи данных между БПЛА и его оператором (это может включать в себя использование протоколов шифрования, таких как SSL и AES), использование техник, связанных с маскировкой IP-адреса, чтобы скрыть фактическое местоположение БПЛА и его оператора (это может включать в себя использование анонимных прокси-серверов или VPN-сервисов), использование программного обеспечения, которое может скрывать свою наличность на дроне, делая его невидимым для антивирусного ПО и других защитных систем, установка программного обеспечения на БПЛА или подсистемы БАС, которое может обеспечить долговременный доступ к управлению (это может включать в себя использование бэкдоров или троянов, которые могут обеспечить удаленный доступ к управлению БПЛА), использование техник, таких как стеганография, для скрытия сообщений и данных внутри изображений и других файлов на дроне, чтобы они могли быть переданы без вызова подозрений
7	Defense Evasion (Преодоление защиты)	Обход защитных мер, которые могут помешать их воздействию на цель. Некоторые из них включают в себя использование скрытых каналов передачи данных для обхода сетевых устройств защиты, использование технологий шифрования данных для скрытия передачи информации от сетевых устройств защиты, маскировка трафика под обычный трафик, чтобы обойти системы обнаружения аномального трафика
8	Command & Control (Получение управления и контроля)	Установление связи с БПЛА и получение контроля над его действиями. Это может произойти, например, вследствие взлома пульта управления БПЛА: злоумышленник может использовать уязвимости в программном обеспечении пульта управления, чтобы получить несанкционированный доступ к управлению БПЛА. Также это возможно из-за перехвата сигнала управления: злоумышленник может использовать специальное оборудование для перехвата сигнала управления, передаваемого между пультом управления и БПЛА, чтобы захватить управление дроном
9	Pivoting (Перехват инициативы)	Туннелирование трафика через контролируемые системы в другие системы дрона, к которым нет прямого доступа для достижения желаемой цели
10	Discovery (Осмотр)	Определение наличия систем защиты и возможных препятствий. Могут использоваться следующие методы: моделирование угроз, использование средств обнаружения и др.
11	Privilege Escalation (Эскалация привилегий)	Получение прав администратора на системе управления БПЛА или на другой целевой системе
12	Execution (Исполнение вредоносного кода)	Выполнение команд непосредственно в БАС для достижения цели
13	Credential Access (Доступ к учетным записями)	Получение доступа к учетным данным, например, логину и паролю для системы управления БПЛА

Окончание таблицы 2

№ п/п	Фаза атаки	Пример атаки
14	Lateral Movement (Свобода действий)	Перемещение между системами, чтобы добраться до целевой системы. Злоумышленники могут использовать различные методы: перехват сетевого трафика между БПЛА и другими устройствами в сети с целью получения доступа к другим системам; использование уязвимостей в программном обеспечении и операционной системе БПЛА для получения удаленного доступа к другим системам в сети; сбор учетных данных и паролей от других пользователей сети с целью использования их для входа в другие системы в сети
15	Collection (Сбор защищенных данных)	Сбор информации о целевой БАС, ее уязвимостях, пользователях при нахождении внутри данной системы, после преодоления систем информационной безопасности
16	Exfiltration (Эксфильтрация)	Извлечение ценных данных или информации из целевой БАС. В контексте атак на БАС эксфильтрация может использоваться для кражи конфиденциальной информации, такой как геолокационные данные, поток данных со станций управления, а также технические характеристики БАС, которые могут быть ценными для конкурентов или других групп интересов. Для эксфильтрации данных БАС злоумышленники могут использовать различные методы: вставку вредоносного кода в систему управления БПЛА, который будет перехватывать и отправлять конфиденциальную информацию на внешний сервер или устройство, эксплуатирующее уязвимости в сетевых протоколах, связанных с БАС, для получения доступа к трафику данных, передаваемых между БПЛА и другими устройствами в сети, установка скрытых программных модулей на БПЛА, которые будут собирать и передавать конфиденциальную информацию на внешний сервер или устройство
17	Impact (Воздействие)	Нанесение вреда или ущерба целевой БАС. Некоторые из методов включают в себя доставку вредоносного программного обеспечения (вирусов, троянов, шпионского ПО и др.), что может привести к манипулированию и уничтожению данных, а также к прерыванию функционирования системы управления БПЛА; использование DoS-атак (отказ в обслуживании), таких как атаки на сеть, при которых злоумышленники отправляют большое количество запросов на целевую БАС, перегружая ее и делая недоступной для легитимных пользователей. Использование атак на физические компоненты БАС может привести к прерыванию работы БАС и потере контроля над ним. Например, злоумышленник может произвести стрельбу по БПЛА, что приведет к его уничтожению, атаки на сетевую инфраструктуру, связанную с БАС, например, на коммуникационные линии, которые используются для передачи данных между БПЛА и станциями управления. Эти атаки могут привести к потере связи и контроля над БПЛА
18	Objectives (Цели)	Достижение конечной цели, которая может быть различной в зависимости от задачи

Преодоление угроз UKC

Преодоление угроз зависит от конкретного контекста и индивидуальных условий. Однако используя модель UKC, можно определить некоторые общие методы и рекомендации по обеспечению информационной безопасности для БАС, которые могут помочь в этом процессе (см. Таблицу 3).

Таблица 3

Общие методы и рекомендации преодоления угроз UKC

№ п/п	Фаза атаки	Общие методы и рекомендации по обеспечению информационной безопасности
1	Reconnaissance (Разведка)	Установление и поддерживание механизмов мониторинга сетевой активности, использование анализа уязвимостей для оценки реального уровня угрозы. Определение наиболее вероятных противников и отслеживание их действий
2	Resource Development (Освоение ресурсов)	Использование многофакторной аутентификации, установка правил контроля доступа, шифрование данных и хранилищ, мониторинг и управление уязвимостями
3	Delivery (Доставка)	Проведение регулярного обучения персонала, установка правил безопасного поведения, использование средств защиты от фишинга и мошенничества
4	Social Engineering (Социальная инженерия)	Использование облачных решений с контролем доступа и механизмами анализа трафика, установка механизмов фильтрации и блокировки подозрительного трафика
5	Exploitation (Эксплуатация)	Мониторинг и анализ сетевого трафика, использование антивирусных программ, обновление программного обеспечения, анализ журналов событий
6	Persistence (Натиск)	Регулярное резервное копирование данных, установка средств защиты от сбоев оборудования
7	Defense Evasion (Преодоление защиты)	Использование многоуровневой защиты, установка систем мониторинга нарушений безопасности, использование интеллектуальных систем обнаружения и предотвращения угроз
8	Command & Control (Получение управления и контроля)	Ограничение доступа к системам управления БПЛА, установление механизмов авторизации и аутентификации для операторов, использование защищенных каналов связи
9	Pivoting (Перехват инициативы)	Наличие системы мониторинга событий, которая будет отслеживать подозрительную активность в сети и своевременно сообщать о ней
10	Discovery (Осмотр)	Наличие системы обнаружения вторжений, которая будет автоматически реагировать на подозрительную активность и блокировать угрозы
11	Privilege Escalation (Эскалация привилегий)	Использование многоуровневых средств обнаружения и предотвращения атак
12	Execution (Исполнение вредоносного кода)	Использование политики наименьших привилегий, регулярное обновление паролей, ограничение доступа к административным функциям
13	Credential Access (Доступ к учетным записями)	Использование механизмов аутентификации, таких как многофакторная аутентификация и шифрование данных
14	Lateral Movement (Свобода действий)	Контроль сетевого трафика и установка ограничений на доступ к сети для некоторых устройств и пользователей
15	Collection (Сбор защищенных данных)	Использование системы резервного копирования данных и механизмов восстановления систем после атак
16	Exfiltration (Эксфильтрация)	Контроль доступа к информации и ограничение ее передачи за пределы системы
17	Impact (Воздействие)	Использование механизмов контроля передачи информации, таких как фильтры сетевого трафика и системы обнаружения утечек данных
18	Objectives (Цели)	Использование системы мониторинга событий и аналитики данных, которая позволит обнаруживать угрозы на ранней стадии и быстро на них реагировать

Это лишь несколько примеров защитных мер, которые могут применяться для минимизации угроз по каждой фазе UKC. Важно также отметить, что эффективная защита требует комплексного подхода и регулярного обновления систем безопасности.

Заключение

Таким образом, использование модели объединенной цепочки враждебных действий (The Unified Kill Chain) может значительно повысить безопасность гражданских БАС и систем воздушного транспорта в целом. Обеспечение безопасности гражданских БАС, включая защиту от различных видов атак, должно быть приоритетом для разработчиков и операторов БПЛА. Однако необходимо учитывать, что безопасность является непрерывным процессом, который требует постоянного мониторинга и обновления. С учетом этого факта применение модели UKC может привести к повышению эффективности систем информационной безопасности БАС и воздушного транспорта в целом. Обмен информацией и совместная работа между различными участниками системы, включая операторов, производителей и правительственные организации, может помочь повысить уровень информационной безопасности воздушного транспорта и предотвратить возможные атаки. Опираясь на модель UKC в создании более надежных и безопасных БАС, данный процесс можно сделать более обоснованным и в конечном итоге построить действительно эффективные механизмы предотвращения атак.

Литература / References

1. Salamh F.E., Karabiyik U., Rogers M.K., Matson E.T. (2021) Unmanned Aerial Vehicle Kill Chain: Purple Teaming Tactics. In: *2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC)*, NV, USA, 2021. Pp. 1081–1087. DOI: 10.1109/CCWC51732.2021.9376090

2. Каталог услуг по информационной безопасности компании «Альтирикс Групп» за 2020 год. Слайд 9. [*Catalogue of information security services of the company «Altirix Groups» for 2020*]. 16 с. URL: https://altirixgroup.com/wp-content/uploads/2021/07/katalog-uslug-ib-altiriks-2020.pdf (accessed 02.04.2023). (In Russian).

3. Willis M., Haider A., Teletin D.C., Wagner D. (Eds) *A Comprehensive Approach to Countering Unmanned Aircraft Systems*. Joint Air Power Competence Centre. 644 p. URL: https://www.japcc.org/wp-content/uploads/A-Comprehensive-Approach-to-Countering-Unmanned-Aircraft-Systems.pdf (accessed 02.04.2023).

4. Pols P. (2017) *The Unified Kill Chain*. Cyber Security Academy. 104 p. URL: https://unifiedkillchain.com/assets/The-Unified-Kill-Chain-Thesis.pdf (accessed 31.03.2023).

5. Choon Seng Tan, Van Bossuyt D.L., Hale B. (2021) System Analysis of Counter-Unmanned Aerial Systems Kill Chain in an Operational Environment. Systems. No. 9. Pp. 79. DOI: https://doi.org/10.3390/systems9040079

6. Best K.L., Schmid J., Tierney Sh., Awan J., Beyene N.M., Holliday M.A., Khan R., Le K. (2020) *How to Analyze the Cyber Threat from Drones: Background, Analysis Frameworks, and Analysis Tools.* Homeland Security Operational Analysis Center operated by the RAND Corporation. URL: https://www.rand.org/pubs/research_reports/RR2972.html (accessed 02.04.2023).

7. Pyzynski M., Balcerzak T. (2021) Cybersecurity of the Unmanned Aircraft System (UAS). *Journal of Intelligent & Robotic Systems.* Vol. 102. Article no. 35. DOI: https://doi.org/10.1007/s10846-021-01399-x