https://orcid.org/0000-0002-5080-1856
https://orcid.org/0000-0003-3604-2256

УДК 004.7

**Ю.М. ЛИСЕЦКИЙ[*], С.И. БОБРОВ[*]**

# SECURITY OPERATION SYSTEM

[*]ДП «ЭС ЭНД ТИ УКРАИНА», г. Киев, Украина

***Анотація.*** *З кожним роком у світі зростає кількість кібератак та кіберзлочинів. Саме тому для захисту від інформаційних та кіберзагроз з'являються нові продукти, технології та інструменти. Одним із найбільш сучасних та надійних інструментів захисту корпоративного рівня є Security Operation Center (SOC). Сьогодні в Україні є вже кілька SOC у державних та силових установах, але питаннями їх побудови цікавляться організації та підприємства майже всіх галузей вітчизняної економіки. SOC дозволяє здійснювати моніторинг, детектування та оперативне реагування на інциденти і, як наслідок, скорочувати шкоду та фінансові втрати, до яких ці інциденти можуть призвести. Треба відзначити, що побудування SOC потребує значних матеріальних витрат, але не всі організації й підприємства можуть їх собі дозволити. Тому питання створення схожого, але доступнішого інструмента, є вельми нагальним. У статті описано Security Operation System (SOS), яка розроблена для ефективного захисту від кіберзагроз і кібератак та призначена для збору, нормалізації, кореляції й аналізу подій у IT-інфраструктурі організації. Основна перевага даної системи – це можливість отримувати інформацію про події з різних джерел і проводити їх кореляційний аналіз, адже сучасні кібератаки та кібезагрози можна виявити тільки за сукупністю подій, що відбуваються в IT-інфраструктурі установи. Ще одна перевага SOS – можливість додавати в аналітичний модуль нові кореляційні правила, які дописують на основі власного досвіду експлуатації системи за результатами аналізу нових атак на IT-інфраструктуру організації та/або за отриманням таких кореляційних правил від інших організацій.*

***Ключові слова:*** *інформаційна безпека, кіберзагроза, кібератака, інцидент, подія безпеки, кореляція, аналіз, IT-інфраструктура, SOC, SOS.*

***Аннотация.*** *С каждым годом в мире увеличивается количество кибератак и киберпреступлений. Именно поэтому для защиты от информационных и киберугроз появляются новые продукты, технологии и инструменты. Так, одним из самых современных и надежных инструментов защиты корпоративного уровня является Security Operation Center (SOC). Сегодня в Украине уже есть несколько SOC в государственных и силовых ведомствах, но вопросами их построения также интересуются организации и предприятия практически всех отраслей отечественной экономики. SOC позволяет осуществлять мониторинг, детектирование и оперативную реакцию на инциденты и, как следствие, сокращать ущерб и финансовые потери, к которым эти инциденты могут привести. Следует отметить, что построение SOC требует значительных материальных затрат и не все организации и предприятия могут себе их позволить. Поэтому вопрос создания подобного, но менее дорогостоящего инструмента, весьма актуален. В статье описана разработанная для эффективной защиты от киберугроз и кибератак Security Operation System (SOS), которая предназначена для сбора, нормализации, корреляции и анализа событий в ИТ-инфраструктуре организации. Основное преимущество данной системы – это возможность получения информации о событиях из различных источников и их корреляционный анализ, так как современные кибератаки и киберугрозы можно обнаружить только по совокупности событий, происходящих в ИТ-инфраструктуре организации. Еще одно преимущество SOS – возможность добавления в аналитический модуль новых корреляционных правил, которые дописываются на основе собственного опыта эксплуатации системы по результатам анализа новых атак на ИТ-инфраструктуру организации и/или по получению таких корреляционных правил от других организаций.*

***Ключевые слова:*** *информационная безопасность, киберугроза, кибератака, инцидент, событие безопасности, корреляция, анализ, ИТ-инфраструктура, SOC, SOS*

***Abstract.*** *The number of cyber attacks and cyber crimes grows every year. This is why there constantly appear new products, technologies and tools for protection against cyber threats. Security Operation Cen-*

*ter (SOC) is one of the most up-to-date and reliable cybersecurity tools of enterprise level. There are already several SOCs in Ukraine in government and law enforcement bodies and there is strong interest to their implementation shown by organizations and enterprises of practically every industry of national economy. SOC allows monitoring, detection and quick response to incidents which is necessary to reduce damage and financial losses caused by such incidents. Implementation of SOC requires significant expenses which can be afforded only by some organizations and enterprises. This is why creation of similar but more affordable tool is very urgent. The paper describes Security Operation System (SOS) designed for effective protection against cyber threats and cyber attacks, which collects, normalizes, correlates and analyses events in organization's IT infrastructure. Main advantage of this system is ability to receive information on events from different sources and their correlation which is important as today attacks can only be discovered on the basis of combination of events in the IT infrastructure. Another advantage of SOS is ability to add new correlation rules into analytical module which can be based on the unique experience of system exploitation, analysis of new attacks against organization's IT infrastructure or borrowing such correlation rules from other organizations.*
***Keywords:*** *information security, cyber threat, cyber attack, incident, security event, correlation, analysis, IT infrastructure, SOC, SOS.*

DOI: 10.34121/1028-9763-2020-2-51-59

## 1. Введение

С каждым годом в мире увеличивается количество кибератак и киберпреступлений [1]. В Украине в последние годы также резко возросло количество преднамеренных вмешательств в работу информационных систем государственных и коммерческих организаций. Практически во всех случаях, после осуществления кибератак, работа организаций была заблокирована от нескольких часов до нескольких дней, что повлекло за собой очень серьезные последствия. Поэтому от степени безопасности используемых информационных технологий сейчас зависят не только стабильность и надёжность функционирования государственных институтов и коммерческих организаций, но зачастую и жизнь многих людей [2]. А для защиты от информационных и киберугроз появляются новые продукты, технологии и решения.

Так, одним из самых современных и надежных инструментов защиты корпоративного уровня является Security Operation Center (SOC). Сегодня в Украине уже есть несколько коммерческих SOC, но вопросами их построения также интересуются организации и предприятия практически всех отраслей отечественной экономики. Такой интерес вызван прежде всего постоянно совершенствующимися кибератаками и потребностью в современном инструменте противодействия им. Действительно, SOC является эффективным инструментом обеспечения информационной безопасности любой организации и позволяет осуществлять мониторинг, детектирование и оперативную реакцию на инциденты и, как следствие, не сокращать ущерб и финансовые потери, к которым эти инциденты могут привести [3]. Следует отметить, что построение SOC требует значительных материальных затрат и не все организации и предприятия могут себе их позволить. Поэтому вопрос создания подобного, но менее дорогостоящего инструмента, весьма актуален.

*Цель данной статьи* – разработка системы, позволяющей организовать эффективную защиту ИТ-инфраструктуры организации от кибератак и киберугроз за счет получения информации о событиях и инцидентах безопасности из различных источников и их корреляционного анализа.

## 2. Системы корпоративной информационной безопасности

Проведенный анализ наличия и эксплуатации промышленных систем информационной безопасности украинскими предприятиями и организациями корпоративного уровня показал, что в среднем используются более 20 классов таких систем (рис. 1).


Рисунок 1 – Системы корпоративной информационной безопасности организации

Это не означает, что все они обязательно должны быть внедрены для достижения «полной безопасности», но это демонстрирует, насколько широк фронт кибервойны и насколько гибко можно формировать ландшафт кибербезопасности, так как для нее уже есть необходимый базис. Конечно, при этом не всем организациям и предприятиям нужен WAF и antiDDoS, не все еще доросли до микросегментации на уровне гипервизора, не у всех процессы требуют/позволяют «ввести» Identity Management.

Вначале следует ответить на вопрос: чем отличаются два понятия – информационная безопасность и кибербезопасность? Ответ можно сформулировать следующим образом: информационная безопасность – это защита данных от различного рода умышленных, неумышленных, природных/стихийных и прочих несанкционированных манипуляций данными (доступ, уничтожение, искажение, препятствование доступу и т.д.), а кибербезопасность – это защита от атак на информационные системы со стороны цифрового пространства.

Таким образом, если информационная безопасность включает в себя резервное копирование, восстановление, архивирование, план непрерывности бизнеса (BCP) и восстановления после катастрофы (DRP), то есть занимается тем, чтобы сохранить корпоративную информацию и возможность ее обрабатывать, то кибербезопасность имеет отношение к таким понятиям, как вредоносное программное обеспечение (ПО), атаки нулевого дня, уязвимость, вектор атаки и т.д. Несмотря на то, что эти понятия достаточно сильно пересекаются, они все-таки имеют определенные отличия и свою специфику. Далее будут рассматриваться именно кибербезопасность и синергия трех ее компонентов: технических средств, процессов и специалистов (рис. 2).

Современные атаки зачастую многовекторные и поэтапные, то есть начинаются с выбора вектора атаки, который даст возможность «пройти» периметр и получить доступ к той или иной информационной системе. Как видно, прохождение периметра сейчас является только первым этапом атаки, а не ее апофеозом, потому что давно прошло то время, когда считалось, что надежный периметр является гарантией безопасности ИТ-


Рисунок 2 – Компоненты кибербезопасности

инфраструктуры, да и само понятие периметра информационной безопасности потеряло свою целостность и монолитность вследствие тенденций развития современных технологий.

Исходя из этого, неправительственная организация MITRE Corporation разработала модель ATT&CK, описывающую этапность, процесс и техники атак и компрометации корпоративных сетей [4]. Согласно этой модели, процесс вторжения и выполнения зловредных действий состоит из нескольких этапов и выглядит, как показано на рис. 3.

Если не учитывать стадию подготовки, то атака состоит из нескольких этапов, которые включают доставку вредоносного контента, заражение, взятие атакованной системы под управление, выполнение разрушающих действий, закрепление и расширение.

По информации от компании-производителя Cisco Systems – мирового лидера в области сетевых технологий, длительность взлома до проникновения составляет минуты, до выполнения вредоносных действий могут проходить минуты, часы и иногда дни, а вот до обнаружения проникновения и результатов атаки проходят недели, месяцы, а иногда и годы.

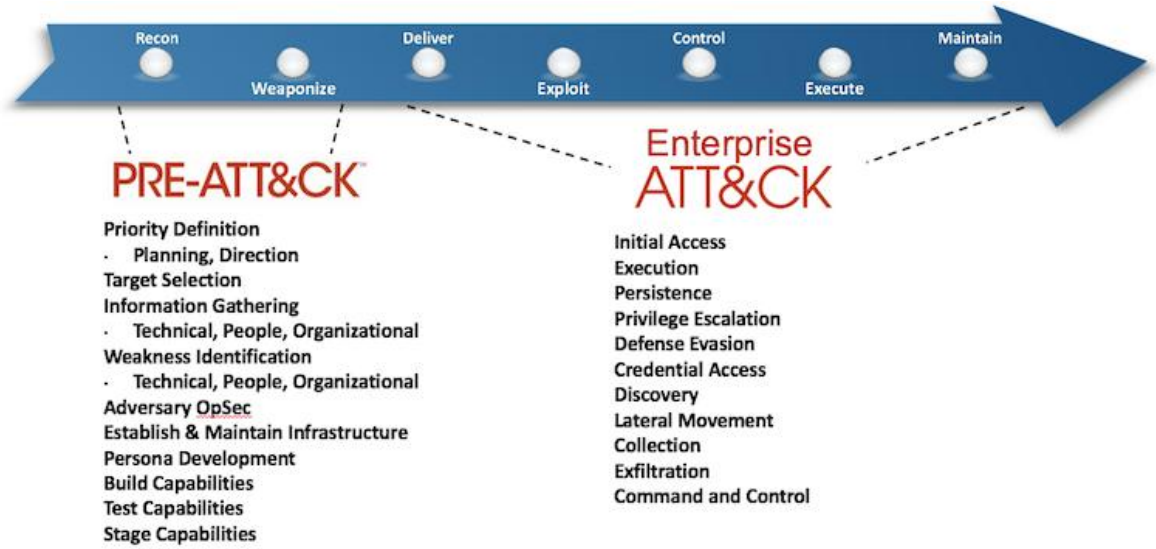


Рисунок 3 – Модель ATT&CK

Из этого следует, что после того, как атакующий, пройдя периметр, уже проник вовнутрь ИТ-инфраструктуры, у защиты есть единицы-десятки минут на то, чтобы предотвратить вредоносные действия, а при все еще существующей концепции безопасности, ориентированной на защиту периметра, до обнаружения проходят месяцы, а иногда и годы.

Для того, чтобы успеть отреагировать на действия злоумышленника внутри периметра, необходимо:

• замедлить злоумышленника, создав для него большое количество ложных целей-приманок в ИТ-инфраструктуре;

• отслеживать активные или вредоносные действия в отношении созданных приманок;

• собрать максимально возможную информацию о сетевом трафике внутри периметра для поиска нетипичного поведения;

• собрать журналы и события ИТ-подсистем, в том числе инфраструктурных и особенно подсистем безопасности;

• провести нормирование, анализ и корреляцию событий и логов;

• выявить нетипичное или опасное поведение и провести расследование и устранение инцидента.

Исходя из вышеописанного, для своевременной реакции на вторжение, когда периметр уже преодолен злоумышленниками, помимо наличия стандартных средств безопасности (антивирус/EPP/EDR, межсетевых экранов следующего поколения, систем безопасности электронной почты и доступа в WEB, систем управлением доступом к сети и пр.) для эффективного отражения современных атак необходимы сбор и централизованный анализ событий внутри ИТ-инфраструктуры.

С учетом того, что в средней сети объем записей о событиях за сутки может достигать десятков гигабайт, просмотр этих событий и их анализ являются весьма трудоемким процессом, что усугубляется различной структурой сообщений, различными уровнями критичности и т.п. Именно для этих целей используются системы Security Information and Event Management (SIEM), задачей которых и является сбор логов с систем, их нормализация, нахождение подозрительных действий и зависимостей для сообщения о них специалисту по безопасности, как о событии удавшемся, неудавшемся или продолжающемся взломе.

Но любое средство сбора и анализа информации не эффективно, если недостаточно информации для анализа. На вход аналитического инструментария должна поступать информация о различных событиях и процессах в ИТ-инфраструктуре. Особенно ценна информация о сетевой активности, найденном вредоносном ПО, срабатывании правил безопасности модулей предотвращения вторжений, а также о срабатывании ловушек-приманок.

Для решения данной задачи необходимо определить минимально необходимый набор систем и устройств, который позволит обеспечить базовый уровень безопасности ИТ-инфраструктуры. Безусловно, что базовый «исполнительный» набор систем кибербезопасности должен также присутствовать в ИТ-инфраструктуре организации. Термин «исполнительный» акцентирует внимание на том, что эти системы исполняют каждая свою роль в решении задачи киберзащиты, и при этом они не обеспечивают дополнительного интегрирующего интеллекта или анализа, а просто защищают конкретные типы систем от конкретных типов атак. К списку таких обязательных систем относятся:

• Logger;

• Next Generation Firewall (NGF)/Intrusion Protection System (IPS);

• Endpoint Protection (EPP)/Antivirus или Endpoint Detection&Response (EDR);

• Netflow collector/analyzer.

Это базовый набор, и он может быть расширен в зависимости от специфики ИТ-инфраструктуры организации и бизнес-задач. Например, если бизнес связан с Интернет или есть портал, то необходимы системы antiDDoS и Web Application Firewall (WAF) при наличии корпоративного WiFi-системы защиты от атак на корпоративный WiFi и т.д. Эти же системы, кроме своих прямых функций, генерируют и передают в аналитическую/коррелирующую систему события безопасности, специфические именно для этой

системы кибербезопасности для объединения в единую базу данных и выполнения анализа.

В качестве централизованного аналитического ядра системы корпоративной кибербезопасности, как упоминалось выше, выступает система сбора и анализа логов и событий – SIEM, которая собирает события из доступного набора систем, нормализирует их и производит анализ, корреляцию совокупностей событий, а также предоставление команде кибербезопасности результатов анализа в виде рекомендаций, выводов и событий.

Для понимания процессов, которые происходят в сети предприятия, данные о трафике (включая данные о 4-ом уровне модели OSI) надо снимать не только с пограничных маршрутизаторов и NGF, но и с сетевых устройств в узловых точках, а для понимания процессов во всех сегментах – желательно со всех сетевых устройств. Примером могут служить данные, получаемые по Netflow, причем необходима информация о всех пакетах, а не Sampled-вариант. Собирать и анализировать всю первичную информацию NetFlow непосредственно в SIEM или предварительно выполнять предобработку Netflow на collector/analyzer, или использовать для анализа систему типа Threat Intelligence с подключением Behavior Analysis и облачных аналитических систем зависит от существующего ИТ-ландшафта, задач, объема сети и типа/интенсивности трафика и выбирается на этапе проектирования.

Для обработки и корреляции событий и процессов в ИТ-системах (сервера, СХД, ОС, приложения,…) необходима обработка журналов событий с приложений, гипервизоров, СУБД, аппаратных платформ и т.п. Для этого такие события могут направляться в SIEM напрямую, а могут осуществляться сбор и предобработка в syslog или SNMP-серверах.

Для выявления фактов успешного вторжения в сеть и идентификации зловредного кода используются системы класса «ловушки», которые провоцируют злоумышленника на активные действия по отношению к созданной обманной псевдосистеме, которая обладает всеми признаками «жертвы», но при этом неизвестна легитимным пользователям и нужна только для того, чтобы отслеживать попытки атак на нее и сообщать системе кибербезопасности детали о злоумышленниках и о типе/способе атаки.

С точки зрения предотвращения взлома ИТ-систем, весьма эффективным решением является анализ ИТ-систем известных уязвимостей при помощи систем класса сканер уязвимости. Такое периодическое сканирование позволяет определить, какие из систем потенциально уязвимы для тех или других классов атак и заблаговременно принять меры для защиты.

Естественно, что чем больше ИТ-систем будут передавать информацию о событиях и активностях системе кибербезопасности, тем более точный анализ будет выполнен и большее количество корреляционных правил будет применено, а это, в свою очередь, позволит команде безопасности обеспечить полную видимость процессов в ИТ-инфраструктуре и действий злоумышленников.

Еще одним компонентом кибербезопасности, как уже упоминалось, являются процессы и процедуры, которые четко описывают для каждого члена команды кибербезопасности процедуры и дальнейшие шаги в случае той или иной ситуации, тайминг и уровни эскалации, процедуры взаимодействия и привлечения специалистов. Процессы и процедуры в службе корпоративной кибербезопасности, как и в любой службе быстрого реагирования, направлены, в первую очередь, на быстрое и эффективное устранение инцидента и его последствий, а во-вторую, не менее важную, на подготовку команды и ИТ-инфраструктуры к работе в постоянно меняющихся условиях, и поэтому делятся, как минимум, на три типа документов: Emergency, Routine, Escalation для каждой усложненной роли специалистов в команде.

Именно специалисты являются самым ценным активом любой службы кибербезопасности. Недаром сейчас в мире наблюдается устойчивый дефицит таких специалистов, который по некоторым оценкам в 2021 г. достигнет 3,5 млн незаполненных вакансий [5]. Без учета этой составляющей наличие большого количества программных и аппаратных средств кибербезопасности не гарантирует безопасность, а в условиях отсутствия реального анализа событий и проведения расследований создает ее видимость.

Как правило, состав команды кибербезопасности определяется на основе штатного расписания и формируется в зависимости от объема ИТ-инфраструктуры, необходимого графика работы команды и требований к компетенции каждого члена команды, а в идеальном случае еще и требования для рекрутингового агентства для поиска специалиста на конкретную роль и разработанного плана обучения для каждого конкретного специалиста.

### 3. Security Operation System

С учетом вышеизложенного, для организации эффективной защиты от киберугроз и кибератак была разработана Security Operation System (SOS), которая предназначена для сбора, нормализации, корреляции и анализа событий в ИТ-инфраструктуре организаций и представляет собой программно-аппаратный комплекс в составе:

• лицензия/подписка на ПО аналитической платформы Splunk Enterprise с модулем Enterprise Security;

• сервер или отказоустойчивый кластер для развертывания аналитической платформы;

• СХД для хранения «глубокого» архива.

Основное преимущество данной системы – это возможность получения информации о событиях из различных источников и их корреляционный анализ, так как современные кибератаки и киберугрозы можно обнаружить только по совокупности событий, происходящих в ИТ-инфраструктуре организации, и практически невозможно по отдельным событиям в отдельных системах информационной защиты (рис. 4).


Рисунок 4 – Взаимодействие SOS с основными системами обеспечения информационной защиты организации

Еще одно преимущество SOS – возможность добавления в аналитический модуль, который содержит более 2000 корреляционных правил (новых) и которые дописываются

на основе собственного опыта эксплуатации системы по результатам анализа новых атак на ИТ-инфраструктуру организации и/или по получении таких корреляционных правил от других организаций.

SOS позволяет реализовывать основные процессы, обеспечивающие киберзащиту:

• сбор логов, Netflow, статистики;
• анализ собранной информации и ее корреляция;
• определение текущих вредоносных действий;
• выявление возможных атак и подозрительных действий;
• формирование реакции на атаки;
• устранение последствий атак;
• устранение обнаруженных «брешей» в безопасности.

Внедрение системы производится в следующей последовательности:

1. Обследование существующей ИТ-инфраструктуры.

2. Прояснение и согласование наиболее опасных векторов атак и наиболее уязвимых/ценных ИТ-ресурсов.

3. Модернизация существующих систем кибербезопасности организации до базового уровня, если необходимо.

4. Установка и инсталляция программно-аппаратного комплекса сбора, анализа и корреляции событий.

5. Разработка и внедрение политик, процессов инструкций, их адаптация для конкретных условий на всех этапах модели ATT&CK (Predict, Prevent, Detect, Response).

6. Обучение штата ИТ безопасности.

Необходимо также помнить, что безопасность – это не состояние, а постоянный процесс адаптации триединой системы (специалисты, процессы, технические средства), который осуществляется итерационно, с целью предотвратить или минимизировать ущерб от вредоносных воздействий на ИТ-инфраструктуру организации (рис. 5).

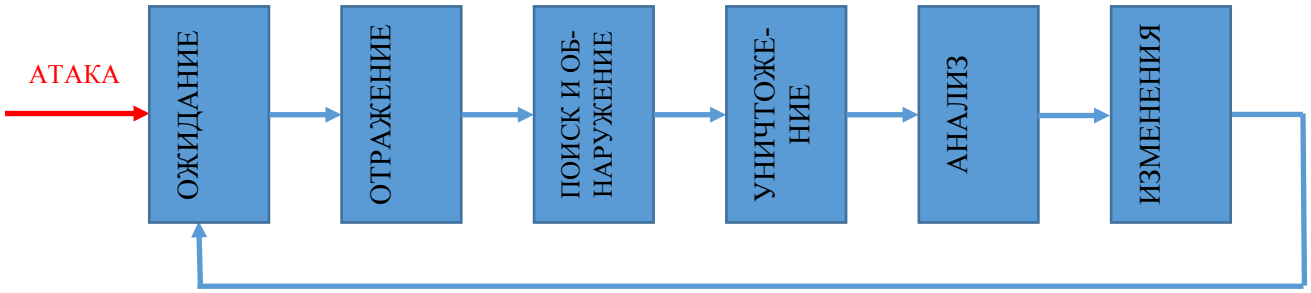


Рисунок 5 – Итерационный процесс адаптации SOS

## 4. Выводы

Таким образом, внедрение SOS позволяет организовать эффективную защиту ИТ-инфраструктуры организации от кибератак и киберугроз за счет получения информации о событиях и инцидентах безопасности из различных источников и проведения их корреляционного анализа. При этом также значительно повышается эффективность анализа событий безопасности за счет обработки аналитиком сразу инцидентов безопасности, а не всего потока журналов событий и Netflow; доступна полная видимость процессов и событий в ИТ-инфраструктуре; появляется возможность анализировать и локализовать инциденты безопасности как внутри, так и на периметре сети; существенно повышается скорость реакции и обработки инцидентов за счет работы команды по разработанным и адаптированным инструкциям и протоколам с четкими ролями.

## СПИСОК ИСТОЧНИКОВ

1. Шейн Х. Кибервойн@. Пятый театр военных действий. Москва: Альпина нон-фикшн, 2016. 392 с.
2. Лисецкий Ю.М., Бобров С.И. Новые угрозы информационной безопасности или оружие массового заражения. *Математичні машини і системи*. 2018. № 1. С. 41–50.
3. Как быстро запустить свой Security Operation Center (SOC). URL: https://www.anti-malware.ru/analytics/Technology_Analysis/How_fast_run_SOC_Security_Operation_Center.
4. ATT&CK for Enterprise Introduction. URL: https://attack.mitre.org/resources/enterprise-introduction/
5. The Mad Dash to Find a Cybersecurity Force. URL: https://www.nytimes.com/2018/11/07/business/the-mad-dash-to-find-a-cybersecurity-force.html.

*Стаття надійшла до редакції 23.03.2020*