IT4Sec Reports 147
http://dx.doi.org/10.11610/it4sec.0147

Каталог от роли на човешкия фактор в киберпространството

Атанас Кузманов,
професор д-р Венелин Георгиев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
и секция „Оптимизация и моделиране“
www.IT4Sec.org

София, ноември 2022

Атанас Кузманов, професор д-р Венелин Георгиев, Каталог от роли на човешкия фактор в киберпространството**,** *IT4Sec Reports 147* (ноември 2022), http://dx.doi.org/10.11610/it4sec.0147

IT4Sec Reports 147 „Каталог от роли на човешкия фактор в киберпространството“ . Идеята за разработване на каталог от роли на човешкия фактор в киберпространството идва от разбирането за това, че от гледна точка на сигурността в двойката човек-компютър по-слабото звено е човека, също така и от това, което клишето казва, а именно че аматьорите атакуват компютрите, а професионалистите атакуват хората. Създаването на каталога от роли предоставя инструмент за постигане на сигурност в киберпространството чрез изучаване и познаване на специфичните характеристики на деструктивните роли и адресираните към тях конструктивни роли на човешкия фактор.

Ключови думи: киберпространство, киберсигурност, конструктивни роли, деструктивни роли, хакери

IT4SecReports 147 „Catalog of human factor roles in cyberspace“ The idea of developing a catalog of human roles in cyberspace comes from the understanding that in terms of security in the human-computer pair, the weak link is the human, and also from what the cliché says, namely that amateurs attack computers and professionals attack people. The creation of the catalog of roles provides a tool for achieving security in cyberspace by studying and knowing the specific characteristics of destructive roles and the respective constructive human factor roles.

Keywords: cyberspace, cyber security, constructive roles, destructive roles, hackers

ISSN 1314-2119

ВЪВЕДЕНИЕ

Проследяването на промените в разбирането за това какво представлява киберпространството дава възможност да бъде разкрита еволюцията в мястото и ролята на човешкия фактор в това пространство. Едни от първите определения за киберпространството се ограничават до разбирането, че то представлява съвкупност от свързани в мрежа компютърни системи или казано по друг начин една отворена мрежа от мрежи. Очевидно на този етап отсъства разбирането, че човешкият фактор е част от киберпространството като се пренебрегват неговото място и роля. На по-късен етап определенията за киберпространството се променят и като пример за това може да бъде дадено определението на ISO, според което киберпространството представлява свързани в мрежа компютърни системи, както и потребителите, а също така и отношенията, в които потребителите влизат помежду си. От този момент мястото и ролята на човешкия фактор в киберпространството стават обект на изследвания и дискусии.

Един от важните въпроси в рамките на идеята за разработване на настоящия каталог е защо е важно да се отчита мястото и ролята на човешкия фактор когато се анализират особеностите на киберпространството. Възможни са различни гледни точки, а от там и различни отговори на този въпрос:

- защото самото киберпространство е създадено от хората и те са онези, които развиват и модифицират неговите характеристики и възможности;
- защото от гледна точка на сигурността потребителите са по-слабото звено в сравнение с компютърните системи и мрежи;
- защото в рамките на киберпространството потребителите могат да играят както конструктивни, така и деструктивни роли и т.н.

Един от възможните начини за изучаване на характеристиките на киберпространството от гледна точка на сигурността е да се направи описание за всяка от възможните роли на човешкия фактор. Събрани в подходящ каталог тези роли могат да бъдат изучавани и анализирани с цел извличане на знания в посока към повишаване на сигурността в киберпространството.

КОНСТРУКТИВНИ РОЛИ НА ЧОВЕШКИЯ ФАКТОР В КИБЕРПРОСТРАНСТВОТО

На първо място в каталога могат да бъдат обобщени и описани т.нар. конструктивни роли. За тях е характерен стремеж към използване и развитие на киберпространството при спазване на съществуващите регулации и противодействие срещу опитите за зловредно използване на киберпространството. В каталога като конструктивни роли са представени следните:

1. *Главен специалист по сигурност на информацията (Chief Information Security Officer - CISO).*[1] Тази роля обобщава част от професионалистите в областта на киберсигурността, в чиито задължения се включва разработване, въвеждане, контролиране и развитие на политиките и процедурите за сигурност на информационните активи. От особена важност за ролята са нивото на академично образование, непрекъснат стремеж за информираност и развитие, знания както в областта на информационните технологии, така и по отношение на мениджмънт, право, управление на човешките ресурси и т.н. Ролята комуникира с главния специалист по информацията (Chief Information Officer - CIO) по

[1] "How to become a chief information security officer," *Cyber Security Education*, 2022, www.cybersecurityeducation.org/careers/chief-information-security-officer/.

отношение на общите ИТ функции в организацията. В неговия фокус са проблемите и решенията на въпросите за сигурността, интегрирани в общите бизнес процеси или как продуктивните бизнес процеси в организацията да бъдат подпомогнати от процесите за създаване на сигурност, в това число и сигурност на информационната инфраструктура. Като допълнително изискване към ролята на главния специалист по сигурност на информацията може да се постави притежаване на определени сертификати (като пример, Certified Information System Security Professional - CISSP), а не рядко и на научна степен. Достигането до ролята изисква преминаване през по-нисши позиции, от които да се натрупа необходимия опит.

2. *Специалист по криптография (Cryptographer).*[2] Във фокуса на тази роля са знанията за алгоритмите и ключовете за криптиране, криптоанализа и системите за киберсигурност. Обхватът на отговорностите включва, но не се изчерпва с участие в създаването на системи за киберсигурност, осигуряване на конфиденциалност на чувствителна информация, анализиране на данни за решаване на проблеми с киберсигурността с помощта на математически и статистически кодове, тестване на системи за киберсигурност за уязвимости, следене за актуални изследвания за изследвания и стратегии за кодиране на приложения и т.н. Ролята изисква съответните технически знания и умения, както и високо ниво на надеждност и лоялност. Като примерни области на необходимо знания за ролята могат да бъдат посочени програмиране, математика, теория на информацията, теория на числата, криптографски алгоритми, хеш функции, структуриране на данни и т.н. Заемането на длъжност, отговаряща на ролята изисква знания в изброените по-горе области, а също така и притежанието на сертификат (като пример Certified Encryption Specialist – CES).

3. *Експерт по криминалистика (Forensics Expert).*[3] Изискванията към ролята реферират към познаване на приложните закони, в частност на закона за защита на личните данни, както и на протоколите за работа с доказателства. Отговорностите на експерта по криминалистика покриват областите за анализиране на инциденти с киберсигурността, определяне на обстоятелствата, събиране на доказателства и тяхното аргументирано представяне в съда. От гледна точка на професионалното образование ролята изисква отлични компютърни умения, познания по право както и за системата за сигурност. Важно условие за изпълняващия ролята е да може да работи бързо и ефективно тъй като често пъти времето се оказва съществен фактор за успеха.

4. *Специалист по тестване за проникване (Penetration Tester).*[4] Изпълняващите тази роля често пъти са наричани етични хакери, тъй като целта им е да откриват уязвимости в компютърните системи. В тази връзка от тях се очаква не само да могат да тестват за проникванията, но и да изготвят доклади, в които да представят резултатите от тестовете си както и съответни препоръки. Тестерите подлагат на изпитание сигурността на системите за да установят ефективността на тяхната защита срещу злонамерени действия. Важно условия за успеха на практикуващите ролята е стремежа за непрекъснато актуализиране на знанията и уменията, познаване на методите за атака, изучаване на нови софтуерни пакети и нови протоколи с цел разкриване на уязвимости. Освен установяването на проблемите, от изпълнителите на ролята се очаква да вземат участие и при тяхното решаване. Изискванията към ролята включват широк спектър от знания и умения в

---

[2] "How to become a cryptographer," *Cyber Security Education*, 2022, www.cybersecurityeducation.org/careers/cryptographer/.

[3] „How to become FORENSICS EXPERT," *Cyber Security Education*, 2022, www.cybersecurityeducation.org/careers/forensics-expert/.

[4] „How to become a penetration tester," *Cyber Security Education,* 2022, www.cybersecurityeducation.org/careers/penetration-tester/.

областите на кодиране, системния анализ, криминалистиката, цялостния бизнес на организацията.

5. *Администратор по сигурност (Security Administrator).*[5] За ролята е характерно поемане на отговорност за познаването, защитата и усъвършенстването на системата за киберсигурност. Отговорностите покриват създаването на изисквания за сигурност, извършване на одити, провеждане на обучения, защита на системата, следене на трафика, разработване на план за реакция и възстановяване при инцидент с киберсигурността и т.н. Като знания и умения ролята изисква академично образование, високо ниво на технически познания, комуникационни умения, отношение към детайлите, концентрация и търпение. Полезни за ролята сертификати се явяват CISM, CISSP, ENSA.

6. *Анализатор по сигурността (Security Analyst).*[6] Ролята покрива отговорности по анализ на политики, процедури и протоколи по сигурността, извършване на одити, предвиждане на заплахи и уязвимости. За заемане на ролята се изисква съответно академично образование, технически умения и комуникационни способности.

7. *Архитект по сигурност (Security Architect)*. Ролята е съществена за ИТ отдела на компанията. Отговорностите покриват проектиране на системи, управление на служители, предотвратяване на атаки, тестване за уязвимости и одитиране. Изисква се академично образование (най-често бакалавърска степен), технически познания, умения за писмена и устна комуникация, иновативна култура.

8. *Одитор по сигурността (Security Auditor)*. Отговорностите на ролята покриват областите за оценяване на сигурността на системите, извършване на периодични тестове, изготвяне на одитен доклад с резултати е препоръки за разрешаване на разкритите уязвимости. Изисква се поне бакалавърска степен в областта на компютърните науки, сертификат за одитор (като пример CISA), определен професионален опит (като пример, пет години в ИТ отдела на компанията).

9. *Консултант по сигурност (Security Consultant)*. Ролята може да се изпълнява от експерт, който работи за различни компании с акцент върху оценката на риска, проблемите и решенията в киберсигурността. Отговорностите покриват полето на анализа и оценката на заплахите от различно естество, инсталиране на устройства за техническа и физическа защита, оценяване на системи за уязвимости и т.н. Ролята изисква минимум бакалавърска степен на образование, набор от специализирани курсове и сертификат (CSC).

10. *Инженер по сигурността (Security Engineer)*. Отговорностите на ролята се свързват със защитата на компютърните системи и мрежи от кибератаки, опазване на чувствителна информация. От заемащите ролята се изисква минимум бакалавърска степен в областта на информационните технологии плюс подходящ сертификат.

11. *Мениджър по сигурността (Security Manager)*. Ролята покрива отговорности, които в по-голямата си част са мениджърски и по-малко технически. Типични задължения са управлението на екипа за киберсигурност, разработването на политики, стратегии и процедури, реакция при инцидент с киберсигурността, създаване на киберустойчивост. Като други ангажименти на ролята са разработването на бюджет и проекти, участие при подбора и назначаването на членове на екипа по киберсигурност, фокусиране на работата на техническите специалисти. Изисквания към ролята се отнасят до наличие на магистърска

[5] „How to become a security administrator," *Cyber Security Education*, 2022, www.cybersecurityeducation.org/careers/security-administrator/.

[6] При описанието на роли от 7 до 15 е използвана информация от *Cyber Security Careers*, 2022, www.cybersecurityeducation.org/careers/.

степен на образование, определен стаж (като пример, пет-шест години), сертификат по мениджмънт (като пример, CISM).

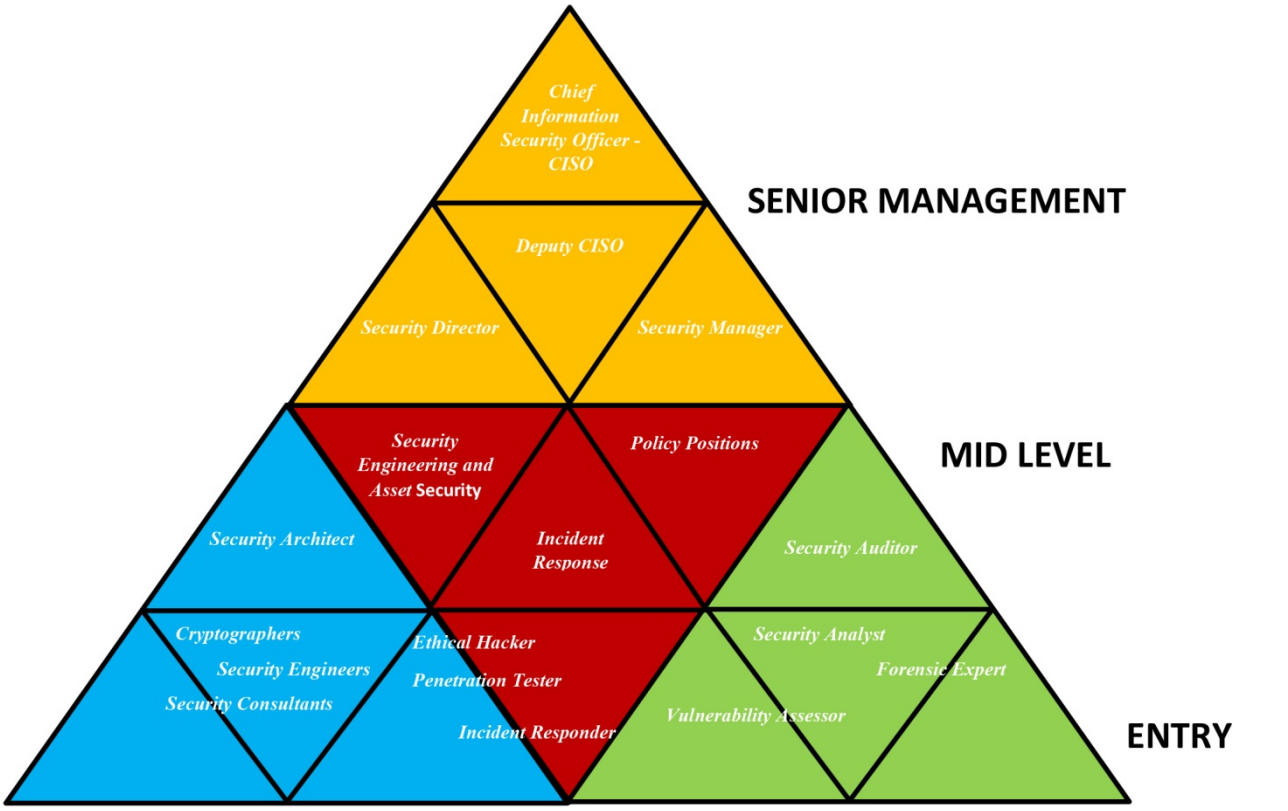
12. *Специалист по сигурност (Security Specialist)*. Отговорностите на ролята покриват поле, включващо защитата на системите от повреди, промени и нерегламентиран достъп, осигуряване на правилно функциониране на информационната инфраструктура, поддържане на актуална информация за актуализациите и промените в системите, разработване на специализирани изисквания, обучение на персонала. Изпълнението на ролята изисква адекватно академично образование, достатъчно стаж и притежаване на сертификати (като пример, ENSA, CCNA). В рамките на ролята може да съществуват специализации то типа на:

- специалист по откриване на проникванията (Specialist in Intrusion Detection);
- специалист по вирусите (Virus Specialist);
- анализатор в център за системни операции (System Operation Center Analyst);
- специалист по възстановяване на данни (Data Recovery Professional).

13. *Одитор на код (Source Code Auditor)*. Ролята се ангажира с преглед на кода на приложенията с цел откриване на грешки, пропуски и уязвимости. Ключов компонент е образованието, което като минимум трябва да бъде бакалавърска степен, допълнено със знания по програмиране, криминалистика, право, криптография, софтуерно инженерство. Като допълнителни изисквания се явяват много добри аналитични способности, прецизност, концентрация, желание за непрекъснато обучение.

14. *Оценител на уязвимости (Vulnerability Assessor)*. Ролята се ангажира с търсене, разкриване и анализиране на слаби места в системите и приложенията. Отговорностите покриват тестване за уязвимости, извършване на одити, сканиране на сигурността, създаване на оценки за уязвимостите, провеждане на обучения и инструктажи на системни администратори. Изискванията към ролята са по отношение на академичното образование, което като минимум трябва да бъде бакалавърска степен, професионален опит плюс релевантни сертификати. Като допълнителни изисквания могат да бъдат посочени нестандартен начин на мислене, ексцентричен подход към стратегии и процедури, прецизност, концентрация, поемане на отговорност и предизвикателства.

15. *Отговорник за реакция при инциденти (Incident Responder)*. Предвид на нейното предназначение, ролята е от особена важност по отношение на сигурността и устойчивостта на системите и мрежите. Отговорностите са в полето на предотвратяване и защитата на атаки и инциденти, както и извличане на поуки от практиката за недопускане на повторни инциденти. От изпълнителите на ролята се очаква да познават грешките и уязвимостите в системите и мрежите, да разработват процедури за справяне с инциденти, да могат да тестват сигурността на системите и мрежите, да планират реакцията при възникване на инцидент. Образованието следва да бъде в областта на информационната сигурност, изисква се определен стаж (като пример, три години) плюс подходящ сертификат от типа на сертифициран анализатор на обратно инженерство, сертифициран етичен хакер, сертифициран тестер за проникванията.



Фиг. 1. Модел за структуриране на конструктивните роли на човешкия фактор в киберпространството.[7]

Сумирането на уменията на конструктивните роли, описани по-горе, изграждат т.нар. човешка защитна стена.[8] Способностите на системите за сигурност да събират и анализират данни стават все по-всеобхватни. Системите предлагат превенция и разкриване на зловреден код, сканиране за вируси, анализ на поведението на потребители, подаване на сигнали при проблеми със сигурността. Тези способности биха били безполезни без хората, които имат знанието за това как да ги внедрят, конфигурират, управляват, развиват и как да ги използват за целите на сигурността. Честа грешка в организациите е дават приоритет на технологиите, а да пренебрегват уменията за тяхното използване. Повишаването на знанията и квалификацията на специалистите по сигурност е не по-малко важно от развитието на технологиите. Човешката защитна стена представлява линията на защитата, която хората създават за да се противопоставят на заплахите за сигурността на организацията. Техническата защитна стена филтрира трафика, а човешката защитна стена представлява човешкия слой на защитата. За човешката защитна стена е характерно:

- не се изгражда само от един човек;
- не се ограничава до екипа за сигурност;
- не е отговорност само на служителите по сигурност;
- не е веднъж завинаги даденост, а се нуждае от постоянно обновяване и развитие;

---

[7] "How to Prepare for a Career in Cyber Security," *Cyber Security Degrees*, 2022, www.cybersecuritydegrees.com/faq/prepare-career-cyber-security/.

[8] Jessica Groopman , "The human firewall's role in a cybersecurity strategy," *TechTarget*, 2021, www.techtarget.com/searchsecurity/tip/The-human-firewalls-role-in-a-cybersecurity-strategy.

Добрата човешка защитна стена изисква осведоменост, обучение, практически навици от страна на всички конструктивни роли и от страна на всички членове на организацията. Модел за структурирането на конструктивни роли на човешкия фактор в киберпространството на базата на равнищата за мениджмънт е показана на фиг. 1.

Човешкият фактор в киберпространството не винаги проявява конструктивизъм по отношение на спазването на регулациите, като следствие от което се появяват деструктивните роли. Примери за подобни деструктивни роли на човешкия фактор могат да бъдат дадени по следния начин:

16. *Субект на заплаха (Threat Actor)*. Ролята обединява субектите, отговорни за инциденти в киберпространството и се използва като неутрален термин, с помощта на който се избягва етикетирането им като отделни индивиди, групи или множества от групи. За ролята не се предписват конкретни технически или други умения и мотивация, както например е при хакерите. Субектът на заплаха е просто субект със злонамерени намерения, който компрометира сигурността на информационните активи.

ДЕСТРУКТИВНИ РОЛИ НА ЧОВЕШКИЯ ФАКТОР В КИБЕРПРОСТРАНСТВОТО

17. *Хакери (Hackers)*[9] най-често се използват като обобщаващ образ за деструктивните роли на човешкия фактор в киберпространството. В средата на миналия век с термина „хакер“ са назовавани специалистите по информационни и комуникационни технологии с богат опит и високо ниво на знания, които са помагали при развитието на технологиите. В последствие терминът разширява своето значение и постепенно се измества в негативната част на разбирането за неговото съдържание. В зависимост от своите цели, мотивация, намерения, степен на знания и опит общността на хакерите може да бъде разделена на различни типове, особеностите на които са представени по-долу за нуждите на каталога от деструктивни роли на човешкия фактор в киберпространството.

17.1.*Хакери с черни шапки (Black hat hackers)*. Ролята често пъти се свързва с криминални хакери и се разглежда като стереотип на киберпрестъпник. Източник на мотивацията най-често е финансовата изгода, но мотивацията може също така да бъде на базата на политически или религиозни убеждения. Като потенциални жертви се разглеждат фирми, държавни институции или отделни потребители. От своя страна хакерите с черни шапки могат да бъдат разделени на следните подкатегории:

17.1.1. *Картечар (Carders)*. За ролята е характерно участие в кражба на информация за кредитни карти с последващи измамни дейности. Не се изискват високи технически умения, а по-скоро умения и готовност за извършване на киберпрестъпни действия.

17.1.2. *Измамници (Scammers)*. За ролята е характерно извършването на различни видове измами: кражба на лични данни, измами със синтетични самоличности.

17.2. *Хакери с бели шапки (White hat hackers)*. По умения тази роля е близка до хакерите с черни шапки, но разликата е на базата на намеренията. Хакерите с бели шапки използват своите знания и умения за да разкриват уязвимости в системите и мрежите и в мерките за тяхната защита, с което да подпомогнат повишаването на ефективността на киберсигурността на организацията.

---

[9] “Types Of Hackers Based On Their Intent: Who Are Ethical Hackers?” UNext Learning, Jigsaw Academy Education, 26 Aug 2022, www.jigsawacademy.com/blogs/cyber-security/different-types-of-hackers/.

17.3. *Хакери с червени шапки (Red hat hackers)*. Ролята е близка до тази на хакерите с бели шапки, но от друга страна са познати като „Робин Худ на хакерството“.

17.4. *Хакери със сиви шапки (Grey hat hackers)*. Ролята включва хакерите, които възприемат своите действия като забавление/развлечение и изпитват удоволствие в разкриването на уязвимости. Рискът при тях идва от това, че изпълняващите тази роля хакват частни мрежи без да имат разрешение.

17.5. *Хакери със зелени шапки (Green hat hackers)*. В тази роля попадат хакерите, които се обучават, т.е. те нямат особен опит, но се стремят да усъвършенстват уменията си.

17.6. *Хакери със сини шапки (Blue hat hackers)*. Ролята е близка до тази на хакерите с бели шапки, с разлика за това че действат след предварително дадено разрешение.

17.7. *Скриптъри (Scrip kiddies)*. Ролята включва лица, които не разполагат със знания и умения сами да разработват зловреден код, а ползват готов такъв.

17.8. *Елитни хакери (Elite hackers)*. Ролята се определя като шампион на съвременното хакерство поради дългогодишния опит на представителите, тяхната висока квалификация, което освен всичко друго им дава възможност да сменят цвета на своите „шапки“.

17.9. *Гейминг хакери (Gaming hackers)*. Представителите на тази роля проявяват интерес към любителите на видеоигри с цел същите да бъдат манипулирани да компрометират идентификационни данни, информация за плащане и други лични данни.

17.10. *Ботнет хакери(botnet hackers)*. Изпълняващите тази роля използват ботнет мрежи за извършване на кибератаки. Ботнетите представляват предварително кодирани подчинени компютърни мрежи, създадени от хакерите за изпълнение на зловредни задачи.

18. *Криптоджакери (Cryptojakers)*. Изпълняващите тази роля най-често се възползват от новости на пазарите на криптовалути за да извършват измами, като пример незаконни искания за плащане с криптовалута в замяна на фалшиви стоки, услуги или инвестиции.

19. *Кибертерористи (Cyberterrorists)*. Ролята включва политически мотивирани киберпрестъпници, които използват своя опит и своята дейност, най-вече чрез разрушаване на информационна инфраструктура, за да привлекат вниманието към своята кауза. Резултатът от тяхната дейност е застрашаване на физическата безопасност на хората и дори загуба на човешки живот.

20. *Злонамерени вътрешни лица (Malicious insiders)*. Ролята покрива лицата, които не се интересуват от качества като честност и справедливост, а умишлено проникват в системи и мрежи на фирмите, за които работят, за да използват добити поверителни данни и информация за извличане на лична финансова изгода.

21. *Хактивисти (Hacktivist*). Ролята покрива лица или групи, чиято цел е да получат нерегламентиран достъп до правителствени мрежи и сайтове, чрез което да постигнат своите политически или социални цели. Много често хактивистите са идеологически мотивирани.

22. *Социални инженери (Social Engineering*).[10] Ролята покрива лица, извършващи злонамерени действия чрез взаимодействие с други лица, определени като жертви на техните атаки. Използват се инструменти на психологическата манипулация с цел да се подмамят потребителите да допуснат грешка по отношение на сигурността, с което тази сигурност да бъде компрометиране, а социалния инженер да постигне своята цел.

[10] “What is social engineering,” *Imperva*, 2022, www.imperva.com/learn/application-security/social-engineering-attack/.

23. *Непреднамерен участник в киберзаплаха (Unintentional cyberthreat actor)*[11]. Ролята покрива онези, които чрез своите грешки създават заплахи за информационната инфраструктура. Допусканите грешки могат да бъдат разделени в две групи:

- грешки на основата на умения, които се състоят в пропуски при изпълнение на познати действия и задачи. В тези случаи крайният потребител знае кое е правилното действие, но не успява да го извърши поради грешка или небрежност. Причина за допускане на грешката може да бъде умора, разсеяност, невнимание;
- грешки на основата на взети решения, които се проявяват когато потребителят взима неправилни решения. Причините могат да бъдат липсата на достатъчно знания, липса на информация, бездействие. Като примери за подобен тип грешки могат да бъдат посочени: слаба защита на паролите, използване на нелегален софтуер, неефективно управление на достъпа.

ЗАКЛЮЧЕНИЕ

Конструктивните и деструктивните роли на човешкия фактор в киберпространството не винаги са директно съпоставими. С развитие на киберпространството деструктивните роли за умножават и модифицират, от което като следствие трябва да се появяват нови конструктивни роли или съществуващите да се модифицират.

[11] Micke Ahola, “The Role of Human Error in Successful Cyber Security Breaches,” *usecure*, 2022, https://blog.usecure.io/the-role-of-human-error-in-successful-cyber-security-breaches.