ЕТИЧЕСКИ МОДЕЛИ НА ДОВЕРИЕ В КИБЕРСРЕДА

ИВАН МИКОВ
Институт по философия и социология, Българска академия на науките
imikov@bas.bg

ETHICAL MODELS OF TRUST IN CYBER ENVIRONMENT

IVAN MIKOV
Institute of Philosophy and Sociology, Bulgarian Academy of Sciences

Abstract
The general idea of this article is to juxtapose three ethical models of trust with the actual problems regarding the use of trust in cyber environment. For this purpose, some key elements from Hume's, Kant's and Nietzsche's ethical theories are used. They are analysed and applied to the concepts of cybersecurity and trust management.

Keywords: trust, security, collaboration, reputation, cyberspace.

Най-непосредствено бихме могли да подходим към проблема за характера и трансформациите на морала в дигитална среда от една консервативна гледна точка. Да заявим, че моралът, ценностите, нормите се трансферират и в киберпространството в пълния си вид, формат и функции, без да търпят някакви промени. На определени структурни нива това би могло да бъде така. Нашето виртуално пребиваване е силно обвързано с наличното ни физическо битие. От друга страна, бихме могли да подходим радикално и да проектираме ако не настоящото, то поне бъдещото еманципиране на виртуалното от реалното, на дигиталното от физическото. Позиция, която е идеал и една от мечтите на трансхуманизма, споделящ очевидно Плотиновия възглед за физическото битие като затвор. В сферата на тези мечти би следвало да се допусне и откъсването на морала(ите) ни от тяхната традиция, от връзката с досегашното прилагане на моралното съдържание и механизми във физическа среда. Да се очаква най-малкото едно същностно преструктуриране на старото, ако не и пълното изначално генериране на някакъв нов морал. Вероятно би било много по-леко, лесно и удобно (в пълен унисон с днешните

ценности) да скъсаме с цялата човешка история и да започнем на чисто в напълно изчислени и подредени дигитални общности с едни съвършено проектирани дигитални тела. Засега обаче за добро или за лошо случаят съвсем не е такъв. Все още ни се налага да се справяме със старите морални проблеми и въпроси, изникващи всекидневно в моралната ни практика. Да се опитваме да търсим нови решения за тях или да актуализираме вече дадените такива, връщайки се понякога към добрите традиции на философията. Поради тази причина ще се опитам да представя проблема за доверието в киберсреда на базата на няколко познати етически обяснителни модела. Практиката показва, че в тази сфера той не просто не е разрешен и изчерпан, а може да се каже, че е съвсем централен за действията и взаимодействията ни в киберпространството. Това прави задачата за пълното му обхващане доста сложна и би следвало да е предмет на едно много по-мащабно проучване, отколкото скромното ми намерение тук.

В случая ще се опитам да ограничa полето на изследването до определен аспект на проявление на въпроса за доверието. За целта ще използвам изходния модел за трите дигитални свята – на потребителя, на разработчика и на техника (по Н. Болц).[1] Последните две зони са тези, които ме интересуват в най-голяма степен, тъй като се отнасят най-пряко до базовата техническа структура на това, което наричаме киберпространство. В този смисъл ако търсим някаква категоризация, може да се каже, че проблемът за доверието ще бъде позициониран в общата сфера на професионалната етика на разработчика. Заедно с това той ще бъде разгледан от перспективите на три класически етически модела и на фона на три може би по-частни, но базови за структурата на дигиталното пространство, критични ситуации в употребата на доверието. Контекстът ще бъде поставен в полето на киберсигурността и по-конкретно в отношение към системите за управление на доверието (*trust management systems*) или на нивата на доверие.

Първата спомената перспектива, на която ще се спра е по-обща и се дава в полето на Кантовата философия. Собствено по проблема за доверието при Кант има тези, разпръснати на различни места в трудовете му. Основната част от тях са в късната му книга *Религията в границите на самия разум* (*Die Religion innerhalb der Grenzen der bloßen Vernunft,* 1793) и са силно обвързани с проблема за вярата. На тази база различни съвременни изследователи правят опити да реконструират една по-цялостна Кантианска

концепция, позиционирана извън религиозните корелации.[2] Оттук се оформят няколко ключови момента. Най-съществено при тях е разделението на двата вида доверие. Най-напред, това е така нареченото от самия Кант *лениво* или пасивно доверие (Kant, 1914: 161; 193). То е свързано с липсата на рефлексия относно собственото морално състояние и постъпки на даден човек. Приемането сякаш наготово и веднъж завинаги на някакъв негов морален облик. Уповаването му на определени външни практики и обичаи за постигане на моралните цели. За Кант човек изпада в самозаблудата, че не са необходими никакви лични усилия и действия за достигането на морално доброто в поведението, а и в живота като цяло. Предпочита да търси заобиколни пътища и да се доверява напълно пасивно на някакви чисто формални процедури, които евентуално да го отведат към благото. Тези характеристики на ленивото доверие Кант свързва първоначално с отношението на човека към Бог. Те обаче са приложими и по отношение на доверието към себе си, а и към другите в обществото (Pedersen, 2012: 153). Например, когато се отнасяме без рефлексия към възможността да се доверим на някого в определена ситуация, приемайки напълно конформистки неговата благонадеждност. Иначе казано, възприемаме човека, на когото искаме да отдадем своето доверие, като напълно предсказуем и предвидим, без търсенето на никакви рационални основания за това. Всъщност, този феномен се обобщава и в мнението, изказано от Артур Шопенхауер: „В нашата доверчивост към другите много често най-голяма част заемат леността, себелюбието и суетата: леността, когато, за да не проучваме, да не следим, да не правим самите ние, с удоволствие се доверяваме на някой друг […]“ (Schopenhauer, 1959: 214). Вътрешен мотив на ленивото доверие е именно желанието да си спестим определени усилия на разума и волята. Пасивното очакване някой да свърши онова, което е в наш интерес. Примесът на егоизъм и суета само засилват неговото въздействие, когато става въпрос за реализиране на нашите собствени дела. Същевременно, според Шопенхауер, доверяващият се очаква неговият жест на доверяване да бъде подобаващо оценен.

Всичко това представлява негативният аспект на пасивното доверие, то обаче може да има и позитивен аспект. Той се свързва с елемента на упражняването на индивидуалните обичайни начини на реакция във всекидневието, придаващи му характера на „съгласувано взаимодействие“. Например, когато сме изправени пред избора дали да се доверим на другите по време на шофиране, по време на пазаруване в

магазина и т.н. (Pedersen, 2012: 154; 158). Реално това включва в своето определение онзи феномен, който обикновено наричаме разчитане или уповаване на някого/нещо. Освен към субекти (хора) то може да бъде прилагано и към обекти (вещи), когато например казваме, че разчитаме на автомобила да издържи дълго пътуване, разчитаме на мобилното устройство да работи без проблеми, разчитаме, че часовникът ни е верен и др. под.[3] Позитивният аспект на пасивното доверие става преходен етап или „условие за възможност на активното доверие“, което е втората форма. При активното или рефлексивно доверие винаги се пита за условията на доверието, за основанията, съгласно които можем да се доверим на другия (Pedersen, 2012: 154). Доверяващият се трябва по пътя на размишлението да достигне до решение дали в даден случай е разумно да се довери или не. Самият Кант акцентира върху необходимостта от личната активност за постигането на моралното добро, като контрапункт на ленивостта (Kant, 1914: 44). Не еднократно действие, а усърдна и непрекъсната работа на човека над самия себе си, основана на рефлексията. Активното доверие и рационалната преценка на другия могат да придобият определени черти на недоверието, но в крайна сметка целта им се свежда тъкмо до установяване на основателно доверително отношение. Както може и да се очаква в една Кантова парадигма, основания да се доверим могат да се намерят. И тези основания са практически, т.е. произтичащи от практическата употреба на разума. От гледна точка на теоретичната му употреба обаче те се разглеждат като хипотетични. На базата на практически основания, които биха могли да са “отделени от изискването за позитивна доказателствена подкрепа“, можем да приемем, че някой ще постъпи според обещанието си, дори да нямаме утвърдително доказателство за това и докато липсва ясен знак, че той няма да го изпълни (Longworth, 2017: 265-67). Този принцип е валиден, докато не е ясно дали другият заслужава нашето доверие. Ако обаче се появи някакво доказателство за обратното, ние рационално ще следва да се съобразим с него. Съответно, да снемем доверието, макар и по-рано вече да сме го били делегирали. Наред с това Кантовата перспектива съдържа и още един компонент. Доверявайки се някому, ние трябва да приемем, че той също се ръководи от моралния закон, когато поема дадено обещание. Пълното следване на закона води до реципрочност на доверието (Pedersen, 2012: 156). Разбира се, този оптимистичен вариант на процеса на доверяване има своите

силно пожелателни нотки. Възможността за реципрочност на доверието трудно може да мисли като предварително гарантирана.

Дотук бяха представени двете основни форми – пасивна и активна, под които може да се подведе отношението на моралния субект при доверителните отношения с другите. Въпросът е как този модел се реализира на практика в киберпространството с оглед на системите за управление на доверието, споменати в началото.[4] В основата стои проблемът за *контрол на достъпа*, като механизъм, чрез който се проверява дали един субект може да манипулира даден обект чрез конкретно действие, т.е. дали има правата, а не вътрешната способност за това. Включен към понятието за доверие този проблем се трансформира в питането: „мога ли да имам достатъчно доверие на S, за да му позволя да извърши действието A с обекта O?“ (Yaich, 2019: 54). Тъй като целта на този механизъм е предпазването на чувствителни/деликатни локални ресурси и данни, то отговорът на въпроса за доверието е от критична важност. Неслучайно в различните му дефиниции и интерпретации в онлайн и киберсреда изобщо, много често присъства елементът на риска. Преекспонират се тъкмо несигурността и неопределеността. Нещо напълно разбираемо, доколкото в киберпространството един от основните проблеми е този с автентичността на идентичностите. Най-общо доверието тук се тълкува като обмислено решение на един субект „да бъде в ситуация на уязвимост спрямо поведението“ на друг субект с оглед на даден проблем в определен контекст (Yaich, 2019: 54). Уязвимостта изразява рисковия компонент на доверието. Свързана е с манипулацията на даден обект или ресурс, вследствие от която би могла да възникне определена вреда или щета за доверителя.

От техническа гледна точна контролът на достъпа, който следва да определя и нивата на доверие има различни форми – базиран на идентичността, решетъчен, ролеви, организационен, атрибутивен.[5] Първата е може би най-познатата от практиката на широката публика, затова ще се спра на нея. Идентичностният контрол на достъпа се реализира чрез два основни метода – удостоверяване на самоличността (автентикация) и упълномощаване (оторизация), които често се припокриват. При тях лицето, искащо достъп, трябва да докаже идентичността си, за да получи права за съответния ресурс. Разрешенията за достъпа са пряко асоциирани с конкретно лице под формата на потребителско име, код за влизане и др. Всъщност тази процедура изпълняваме

всекидневно, използвайки своите електронни пощи, облачни хранилища, профили в социалните мрежи, профили в онлайн магазини и т.н. По същността си освен технически взаимодействия това са и взаимодействия на доверие, при това *двустранни*. Потребителите се доверяват на разработчика, платформата или най-общо казано на услугата като предоставят своите лични данни, разчитайки те да бъдат съхранявани добросъвестно. Разработчиците, от своя страна, се доверяват на потребителите, като им предоставят достъп до своя продукт и ресурси с презумпцията, че те ще бъдат използвани без злоупотреби.

В този момент обаче можем да отбележим и вече посочените две Кантови форми на доверие. Пасивното доверие се проявява особено често в киберсредата, свидетелство за което са множеството злоупотреби с потребителски лични данни, профили, пароли. От страна на потребителите пасивното или ленивото доверие води до понижено внимание при ползването на дигиталните ресурси. Например, при посещаване на уебсайтове с липсващи или невалидни сертификати за сигурност, когато не се проверява тяхната изрядност и се въвеждат лични данни и пароли, отговаряне на *fishing* писма, отново без проверка на източника. С намерението да изпълнят действието, което са си набелязали потребителите често игнорират предупрежденията за сигурност, свалят или отварят файлове с вируси. Станалите широкоизвестни случаи отпреди няколко години с компютърните вируси *WannaCry, Petya/NotPetya, BadRabbit* са показателни в този смисъл. Предоверяването на онлайн ресурсите е пряко следствие от ленивото доверие. Обратно, вниманието и проверката при употребата на предоставяното онлайн съдържание, сочат за действието на активно потребителско доверие. От страна на разработчиците и предоставящите онлайн услуги пасивното доверие води до появата на проблема с фалшивите профили, особено в социалните мрежи.[6] Най-често това се случва, когато при основния процес на създаване на такива профили липсва допълнителна проверка на идентичността. Разбира се, с уточнението, че няма пълни гаранции, че и тя не може да бъде заобикаляна. Проблемът с фалшивите и спам акаунти реално стои и в основата на този с фалшивите новини. Те се генерират и разпространяват посредством подобни неавтентични идентичности. Значимостта на предотвратяването и на двете е очевидна. За проява на активно доверие пък могат да бъдат посочени извършваните проверки от платформите и разработваните от тях допълнителни системи

за верификация (например, най-масовата двустепенна автентикация чрез мобилен телефон или приложение). Също така, използваното най-вече при електронната търговия обвързване на даден потребителски профил с банкова карта.

Ако се върнем отново към споменатата вече система за управление на доверието, то тя може да се дефинира като: „абстрактна система, която обработва символната репрезентация на отношението на доверие от перспективата на автоматизацията на вземане на решение за доверяване“. Това ще рече, че доверието преминава през събирането и обработката на информация, целящи осигуряването на достъп, делегирането на права и колаборацията (Yaich, 2009: 63-4). Тъкмо последният посочен елемент – колаборацията (сътрудничеството), е ключов и ни препраща към втората перспектива или втория етически модел на доверие. Връзката между доверието и сътрудничеството е набелязана в един емблематичен и често цитиран пример на Дейвид Хюм от Третата книга на неговия *Трактат за човешката природа*, който е следният: „Двама съседи биха могли да се споразумеят да отводнят една ливада, която и двамата притежават общо, защото за тях е лесно да разберат своите намерения и всеки от тях трябва да схване, че непосредственото следствие от неуспеха в неговата част, ще бъде изоставянето на целия проект“ (Hume, 1985: 590). Основното са именно непосредственият интерес и изгодата за двете страни, които обосновават за тях решимостта за действие и стават двигател на доверието. Успешната колаборация е възможна само при пълното изпълняване на ангажимента от всяка страна, свързан със зададената обща цел. А доверието, което се отдава, следва да е реципрочно.

Как обаче този модел на колаборация обяснява проявата на доверие в отношение към дигиталната система за управление на доверието? Тя най-общо казано съдържа три основни елемента: дигиталните удостоверения (*credentials*), политиките (за достъп, *policies*) и доверяващи машини (*trust engines*). Последните представляват алгоритмите, чрез които се автоматизира процесът на сверяване и оценяване на съответствията при идентификация, но решенията за доверяване се взимат от човек или от приложението, което ги ползва, не от системата (Yaich, 2009: 65). Вторите съдържат видовете разрешения, които могат да се дават на всеки субект за достъп до ресурсите. За нас в случая от особен интерес са тъкмо първите – удостоверенията, които са символните репрезентации на доверието. Те са в центъра на *взаимодействията* в киберсредата и

съответстват на тези във физическия свят, например, лични карти, шофьорски книжки, карти за ползване на транспорт, карти за библиотеки и др. под. Дигиталните удостоверения са от една страна споменатите вече сертификати за сигурност, издавани от определени институции (по стандарта X.509), наречени удостоверяващи центрове (*certificate authorities*). Те съдържат пълната информация, идентифицираща притежателя им, съответно уебсайт на организация или отделно лице. В доверително отношение влизат потребителят и предоставящият услугата, но опосредствано чрез авторитета на удостоверяващия център. Най-малката полза от тези сертификати, която би могла да се спомене, е предотвратяването на хакерската атака „човек по средата“ *(Man-in-the-middle*), при която може да бъде прихваната и подменена лична информация. От друга страна, обаче, по-интересен от наша гледна точка е случаят с т.нар. крос-сертифициране, в основата на което е инфраструктурата на публичните ключове, по известна като PGP (*Pretty Good Privacy*). Тя е особено разпространена в сферата на такива всекидневно употребявани услуги като електронните пощи и чатовете.[7] При нея всеки един субект може да издаде свой собствен сертификат, действайки по този начин като удостоверяващ център и да сертифицира, т.е. да подписва публичните ключове на другите. Всеки потребител разполага с два ключа: публичен и частен. Публичният ключ се разпространява и предоставя на другите потребители, за да могат те да шифроват съобщенията до притежателя му, които той впоследствие разшифрова чрез своя частен ключ, пазен секретно. Валидирането на публичните ключове е в основата на въпроса за доверието при *PGP* сертификатите. Затова са установени три модела на доверие или доверително взаимодействие – директно, йерархично и „мрежово“ (вж. Callas, 2008; Ryabitsev, 2015). При директното, двама потребители се срещат лично във физическия свят и обменят „на живо“ своите ключове. Тъй като често е трудно един потребител да се срещне в такава форма с всичките си онлайн контакти, често се организират специални „партита за подписване“, където става масовата размяна/подписване на ключовете. В този смисъл една от основните пречки пред функционирането на доверието в киберсредата е тъкмо удостоверяването на самата физическа идентичност на другия и проблемът дали зад нея стои реална личност. Нещо, което в ситуации от физическата реалност няма толкова голяма тежест. Йерархичното доверие е свързано с приемането на сертификати на пряко непознати потребители на базата на общи познати, които вече

са удостоверили техните ключове, т.е. използването на една верига на доверието. Тези два модела са обхванати в най-мащабния – т.нар. м*режа на доверието* (*web of trust*). При него доверието се натрупва чрез преплитането на различни вериги от потребители, удостоверяващи един другиго. В киберпространството действат множество такива мрежи на доверието, които се обвързват взаимно. От основната причина и цел на тяхното съществуване, а именно сигурната комуникация с другите в онлайн пространството, се демонстрира Хюмовият пример за съседите. Защото размяната на шифровани електронни писма и чат-съобщения има своя смисъл само и единствено при равното съучастие на страните. Ако един от двамата кореспонденти не шифрова собствените си съобщения, той излага на риск и съобщенията на другия. Шифроването работи чрез споделено доверие, че другият също ще шифрова съдържанието. Водени от общия им интерес, както твърди и Хюм, двамата потребители вече знаят какво следва да направи всеки, за да не пропадне цялото им начинание. Взаимодействието и сътрудничеството тук са от абсолютна важност.

И накрая вследствие от разгледаното дотук се очертава третата перспектива към проявата на доверието в киберсреда. Тя се разкрива в казаното от Ницше, във втория раздел на *Генеалогия на морала,* по повод формулировката му за човека като „животно, което може да обещава“. Проблемите за обещанието, отговорността и съвестта са разгледани като пряко обвързани с този за доверието. Процесът на култивиране на човека като такъв, който може да поема и спазва обещания е интерпретиран като механизъм, насочен към превръщането му в предвидим, изчислим, правилен, необходим. За Ницше посредством продължителната работа на обществото и чрез особената възпитаваща сила на „нравствеността на обичаите“ (нравите, *Sittlichkeit der Sitte*) се достига в резултат до един „суверенен индивид“ със свободна воля. Той е способен да гарантира за себе, да поема и изпълнява обещания, въпреки всички трудности. Свободният индивид признава и уважава равните на него, предизвиква доверие у другите, но сам трудно се доверява (вж. Nietzsche, 1988: 291-94).

С така накратко изложената концепция следва да се подчертае още едно измерение на доверието. Тя поставя пряко въпросът за неговата връзка с добрата репутация, престижа. Най-безпроблемно и без (или с минимален) риск доверието може да бъде отдадено именно на онзи, чиято репутация е широко призната, доказана и

утвърдена според общото мнение, общността. Добрата репутация говори сама за онзи, който я притежава, прави го сигурен, надежден. Трябва да се отчита и фактът, че репутацията – формална (базирана на обективни механизми и системи) или неформална (базирана на слухове и мнения) – може да бъде многомерно повлияна от различни предубеждения и предразсъдъци, срещу които обаче са налични и потенциални корективи (Orrigi, 2020: 93; 95). Прозрачността, свободният достъп, отвореният код са само някои от тези корективи и опции за контрол върху евентуалните манипулации с репутационните системи. Механизмите на формалната репутация имат непосредствено влияние върху установяването на доверието в киберсредата. Един техен аспект са разгледаните „мрежи на доверие“ (Seigneur, 2009: 82). Потребителите с повече подписи на своите сертификати притежават и най-добра репутация, реноме. Те са тези, които създават най-големи вериги на доверието, разширяващи всяка мрежа. Подписаните от тях сертификати са гарантирани като сигурни. По същия начин наличието на професионални и бизнес сертификати на уебстраниците потвърждава тяхната сигурност чрез добрата репутация на удостоверяващата инстанция. Недобър подход, например, за бизнес сайтовете с множество потребители се смята използването на самоподписани и безплатни сертификати.

За контрол на нивото на репутацията се разработват и въвеждат т.нар. „системи, ръководени от репутацията“ (*reputation-driven systems*), разчитащи на качествени, а не количествени показатели, за да култивират доверието сред онлайн общностите (Kwan and Ramachandran, 2009: 293; 309). Те използват различни технически инструменти и механизми, за да ограничават рисковото поведение на потребителите, да стимулират и засилват отговорността и сигурността. Някои от тези инструменти включват писането на коментари към потребителски профили, даването на обратна връзка (*feedback*), създаването на рейтинги на потребители от потребители, изключването на възможността за анонимна активност в онлайн платформите. Тези подходи са особено забележими при онлайн търговията, на сайтове като *Amazon*, *eBay*, а и техните локални алтернативи. Наред с това и пряко при разработчиците на различни програмни продукти доброто ниво на обратната връзка и оценките на потребителите влияят върху нивото на репутацията на съответния разработчик и търсенето на неговите продукти. Реципрочно, препоръката, която може да даде разработчик или организация с висока репутация влияе на

позитивния образ на препоръчваното. Ориентирането на потребителя, проверката на рейтинга и съответно репутацията на разработчика е още една проява на активно доверие.

В обобщение може да се каже, че доверието в киберсредата се проявява като свързващ елемент между трите дигитални свята. На базовото ниво на функциониране на киберпространството основен проблем се оказва неговата взаимовръзка с проблема за сигурността. От тази корелация произтичат редица съпътстващи въпроси като тези за идентичността, колаборацията и репутацията в дигитална среда. В основата на техните морални измерения се позиционира доверието, което придобива допълнителни характеристики от спецификата на киберпространството, свързани с автоматизацията, валидирането, удостоверяването. Етическите модели предлагат различни теоретични оптики за осмислянето и овладяването на тези феномени и процеси.

БЕЛЕЖКИ

[1] До известна степен темата, която разглеждам тук се явява продължение и част на едно по-цялостно изследване върху функционирането на морала в дигитална среда. В този смисъл се позовавам на тризоновия модел на Норберт Болц и в преходните ми проучвания, вж. Bolz, N. (2007). *Das ABC der Medien*. Wilhelm Fink Verlag, München.

[2] Сред основните имена, на чийто опити за реконструкция се спирам тук са Естер Педерсен и Гай Лонгуърт.

[3] Вж. Ess, 2020: 408, където се разграничават *довериeто* и *разчитането* (*reliance*), като последното е отнесено към „обектите и машините“, при които отсъства способността за избор. От своя страна Педерсен предлага едно снемане на „разчитането“ в понятието за доверие, като го прави съществен етап от пасивното доверие.

[4] Използваните по-долу технически обяснения и примери нямат за цел да предоставят изчерпателно и стриктно техническо изложение. Имат по-скоро функционално значение с оглед на съпоставката им с разглежданите морални понятия.

[5] За по-пълно обяснение на различните модели вж. Yaich, 2009: 54-61.

[6] Не е тайна сериозното разпространение на проблема с фалшивите идентичности в такива социални мрежи като *Facebook* и *Twitter*, въпреки усилията за ограничаването им.

[7] Някой от най-популярните сред тях са *Protonmail, Mailbox, Tutanota, Telegram, Signal* и др. Те предоставят възможност за изпращане и получаване на шифровани имейли и съобщения, повишаващи сферата на защита на личната информация.

ЛИТЕРАТУРА

Callas, J. (2008). *An Introduction to Cryptography*. PGP Corporation.

Ess, Ch. (2020). Trust and Information and Communication Technologies. In: *he Routledge Handbook of Trust and Philosophy*. New York and London, Routledge Taylor & Francis. pp. 405-420.

Hume, D. (1985). *A Treatise of Human Nature*. London, Penguin Books.

Kant, Im. (1914). *Die Religion innerhalb der Grenzen der bloßen Vernunft*. In: Kant's gesammelte Schriften, Bd. VI. Berlin, Verlag G. Reimer.

Kwan, M. and D. Ramachandran (2009). Trust and Online Reputation Systems. In: *Computing with Social Trust*. London, Springer Verlag, 287-311.

Longworth, G. (2017). Faith in Kant. In: *The Philosophy of Trust*. Oxford University Press, pp. 251-271.

Nietzsche, F. (1988). Zur Genealogie der Moral. In: *Kritische Studienausgabe*, Bd. 5. München/Berlin/New York, dtv/de Gruyter. 245-412.

Origgi, G. (2020). Trust and Reputation. In: *The Routledge Handbook Of Trust And Philosophy*. New York and London, Routledge Taylor & Francis. pp. 88-96.

Pedersen, E. (2012). A Kantian Conception of Trust. In: *SATS - Northern European Journal of Philosophy*, vol. 13, no. 2, 2012, pp. 147-169.

Ryabitsev, K. (2014). *PGP Web of Trust: Core Concepts Behind Trusted Communication.* Available at: https://www.linux.com/training-tutorials/pgp-web-trust-core-concepts-behind-trusted-communication.

Schopenhauer, A. (1959). *Aphorismen zur Lebensweisheit*. Stuttgart, Alfred Kröner Verlag.

Seigneur, J.-M. (2009). Social Trust of Virtual Identities. In: *Computing with Social Trust*. London, Springer Verlag, pp. 73-118.

Yaich, R. (2019). Trust Management Systems: A Retrospective Study on Digital Trust. In: *Cyber-Vigilance and Digital Trust. Cyber Security in the Era of Cloud Computing and IoT*. London, ISTE Ltd and John Wiley & Sons, pp. 51-104.