Астра Манасиева

КИБЕРПСИХОЛОГИЯ
ПОВЕДЕНЧЕСКИ АСПЕКТИ

София, 2016

ISBN 978-619-152-896-7

Д-Р АСТРА МАНАСИЕВА

КИБЕР-ПСИХОЛОГИЯ

ПОВЕДЕНЧЕСКИ АСПЕКТИ

ИЗТОК ЗАПАД

На съпругът ми Кирил
за съпричастността, обичта и подкрепата!

Съдържание

Част III.
Поведенчески характеристики на извършителите на компютърни престъпления / 111

Благодарности

Бих искала да изкажа дълбоката си благодарност и признателност за подкрепата, разбирането и мотивацията, дадени от моя научен ръководител по време на следването ми – проф. Бойко Ганчевски и за помощта, насоките и критичните бележки, който ми даваше по време на писането на дисертационният ми труд, част от които по-късно са представени в настоящата книга. Благодарение на ерудицията, високият професионализъм и персоналните му качества за мен бе изключително удоволствие и привилегия да работя с него и да съм негов докторант.

Също така бих искала да изкажа благодарност на проф. Снежана Илиева от СУ за мнението, анализа и подкрепата, като съм поласкана от високата оценка дадена от нея относно работата ми и съм впечатлена от прецизността, професионализма и насочеността, с които работи.

Изказвам и дълбката си благодарнст на проф. Стефан Мичев, доц. Иво Великов, колегите си от АМВР и СУ, проф. Валери Стоянов, проф. Георги Петков, Асен Ташев, Михаил Петров и на всички за мен невероятни хора, с които имах честта да се запозная и да работя и които ме мотивираха и продължават да ме мотивират в професионалният ми път.

Благодарение на тях и на съветите, експертното им мнение, приятелството, насоките и помощта тази книга стана реалност и не остана поредната нереализирана идея.

Признателна съм на моето семейство и особено на съпругът ми Кирил за вярата, за това, че в нито един момент не се усъм-

ниха в мен, а напротив – в етапи, в които самата аз губих вяра и поглед, успяваха да ме върнат в реалността и да ми покажат вярната посока.

На съпругът ми, който ми даде куража да реализирам идеите си и който не престана нито за миг да вярва в мен. Без неговата неотлъчна подкрепа, оптимизъм и вяра не бих имала смелостта да съм това, което съм!

Благодаря ви!

Въведение

Престъпността в сферата на компютърните технологии взима все по-високи темпове на разпространение и развитие. В един съвременен свят технологизацията, а с това и навлизането на иновативни модели и компютъризацията са от основно значение за развитието на обществото.

Честото изменение на традиционната престъпност в онлайн такава прави проблема за компютърните престъпления и тяхното разпространение и разрастване все по-актуален, а оттам следва и необходимостта от неговото разглеждане. Това определя и предметът на настоящата книга, а именно – извършителите на различни компютърни престъпления, като обект на анализ е техният психологически профил.

Чрез незаконното пробиване и завладяване на компютърни данни извършителят, манипулирайки с информацията извлечена от тях, може да окаже както физически, така и психически тормоз върху жертвата си като границите на това варират и зависят както от личната мотивация и поставените ограничения, така и от отношението на самия потърпевш и начина, по който извършителят приема, че той го предизвиква, стимулира, блокира или отговаря на тези атаки.

Основният отличителен белег на правонарушителите в сферата на компютърните технологии е притежанието на познания и умения в тази област. Това са качества, без които извършването на този тип престъпления не биха могли да се осъществят. Но освен овладяването на определени познания за осъществяване

на този тип криминални деяния са необходими и конкретни мотиви и начини за извършване. Точно те биха дали по-пълна и точна представа за това какво различава този тип извършители от останалите.

Тъй като компютърът се приема и за средство и за начин на извършване на противоправното деяние, то от значение за психологическия портрет на извършителите е да се разберат и анализират техните мотиви и желания, подтикващи ги точно към този вид престъпност, а не към друга.

Интерес представлява да се изведат основните начини за извършване, характеристиките и моделите, от което и да се обособят най-разпространените видове киберпрестъпници, а именно: хакери, различен тип крадци (на финансови средства, самоличност, интелектуална собственост), както и извършители, които злоупотребяват с информация в различен тип социални мрежи – разпространение на вируси и зловреден софтуер, манипулация и измама с лични данни, както и разпространение на детска порнография и пиратство.

През последните години все по-чести стават и компютърни престъпления, свързани с кибертероризъм, шпионаж, следене, дебнене и различен тип тормоз върху набелязаните жертви. Всичко това води до един глобален проблем, който се разраства с всеки изминал ден и чиито последици могат да бъдат пагубни.

Чрез манипулиране на определен тип информация, извършителите на изброените престъпления търсят удовлетворение на собствените си цели, подбуди и мотиви. Независимо дали в по-голям процент от случаите става въпрос за користни подбуди или такива на себедоказване чрез отделни агресивни методи и атаки – този тип индивиди са интересни от гледна точка на профилиране, тъй като освен заплахата, която представляват, основната теза от която се изхожда е че притежават определени личностни характеристики, които ги отличават от останалия тип извършители на криминални деяния.

Към момента както на национално, така и на международно ниво постоянно има случаи на компютърен саботаж, шпионаж, кибервойна, социален инженеринг, пробиви и атаки от хакери,

незаконно използване на компютърни системи и мрежи в големи корпорации, болници, правителствени институции, университети, кражба на патенти, авторски права, модели и дизайни, източване на сметки, смяна на самоличност, увреждане на лични данни и спекулиране с тях, качване на порнография (както детска, така и за възрастни), експлоатиране на различен тип потребители, мониторинг на определени хора, разпространение на вредоносни програми, вируси и др., на които се гледа като на новини като малко са тези, които оценяват заплахата от потенциални престъпни прояви и злоупотреби.

С все по-голямата технологизация и отдалечаването на хората в междуличностните им взаимоотношения един с друг, онлайн комуникацията започва да измества реалната, като и начините за връзка с околните започват все повече да се свеждат до виртуалното общуване. Така и голяма част от традиционните престъпления, като измама, рекет, обир и др. започват да се преобразуват в онлайн престъпност, криеща в себе си дори по-голяма опасност от реалната. Психологическият натиск върху жертвите е също толкова силен и опасен, както и ако има реален контакт с тях.

Създаването на един обобщен профил на киберпресъпниците – против личността и против собствеността чрез наблягане на психологическия аспект на начинът по който се извършват основните видове компютърни престъпления е основен акцент на тази книга. Чрез анализ на случаи, примери, подбор на модели, теоретични постулати и различен тип типологии и класификации се търси да се изведат онези аспекти от профилните характеристики на тези лица, които биха дали по-ясна и прецизна представа за самите тях, техният профил и личностни предиспозиции. Това би помогнало и за излагането на някои препоръки относно превантивната мярка срещу тях.

Целта на тази книга е да запознае читателите с начините на извършване на този тип престъпления, а оттам и да интерпретира и изведе основните психологически характеристики на правонарушителите, вниквайки по-дълбоко в тяхната ценностна система и мотиви. Нещо, изключително необходимо, но малко акцентирано от гледна точка на анализ и разследване.

Чрез интерпретация на видовете извършители и методите им на действие, техните нагласи и подбуди, начина за избор и манипулация на жертвите, както и последиците върху последните се цели един по-конкретен психологически профил на киберпрестъпниците като по този начин актуалността на проблематиката би могла да се сведе обобщено до научна и практическа. Чрез първата бих се надявала книгата да допринесе в теоретичен план чрез своите анализи и обобщения, а чрез практическата– да има реално приложение главно чрез превенция и намаляване на този тип престъпност, както и в оперативно-издирвателния аспект.

Обектът на изследване са самите извършители разделени на две групи – против собствеността и против личността. Целта е да се предаде подробна теоретична рамка, в която да се опишат отделните модели и теории, водещи до девиации, което от своя страна би помогнало за анализ на поведението на извършителите. Освен това е необходимо да се наблегне на основните методи и начини за извършване на конкретните престъпления. Това ще даде по-точна представа за техните психологически и личностни характеристики.

По този начин биха се изяснили причините, мотивите и начините на действие, а оттам би следвала интерпретацията им и създаването на психологически профил. Важно е да се даде отговор на въпроса какво точно мотивира и предизвиква определени хора да извършват този тип криминални деяния, а други – не. Смятам, че с анализ на случаи, примери и литература, както и че с извеждане на профили на изследваните лица би се получила по-ясна картина относно поведенческите им характеристики и подбуди.

Задачите, които се опитвам да разясня в рамките на тази книга се свеждат до:

- да се открият, анализират и обобщят онези личностни качества, които могат да бъдат индикатор и водещ мотив за киберпрестъпност;
- да бъде разгледана виктимологията и последиците върху жертвите;

- да се направи общ преглед както на теорията за криминалното поведение, така и на правната регламентация на този тип престъпност;
- да се разгледат главните видове компютърна престъпност и начините за нейното извършване, както и извършителите, някои случаи, изводи и статистически данни;
- да се изяснят мотивите на киберпрестъпниците, техния темперамент, нагласи, когнитивни и емоционални компоненти или да се направи профил на този тип извършители
- да се изведат основни изводи и обобщения от цялостния теоретичен и практичен анализ.

Използвала съм като основно средство мета-анализ на случаи и литература, който ще помогне за навлизане в тематиката и който ще предостави възможност за получаване на допълнителна информация, както и за запознаване със спецификите на проблематиката.

Смятам, че сравнителен анализ между България и Англия в начина на двете страни за разкриване на този тип престъпления, както и последваща работа на оперативните органи би дал поясна прецизност за мястото на страната ни в борбата срещу киберпрестъпността.

Всичко това се прави с цел запознаване на читателят в проблематиката, неговата информираност, запознаване и изясняване на някои аспекти от тази трансгранична, многопрофилна и изключително опасна престъпност, разрастваща се стремглаво и оказваща влияние в почти всеки един сектор от екзистенцията и начина ни на живот – както на индивидуално, така и на организационно ниво.

Част I

Киберпсихология в контекста на криминалната психология

Глава първа

Профилиране в криминалната психология

1. Същност на психологическият профил

Темата за личността на престъпника вълнува както обществото като цяло, така и органите, които се опитват да се справят с нейните криминални прояви. Това е проблем, в който се вплита комплекс от криминологически, социологически, психологически, юридически, педагогически, етични и други фактори.

Обособяването на личността на престъпника като предмет на познание от криминалната психология предполага да се определи какво точно се включва в нея – кои са подбудителните ѝ мотиви, както и как те оказват влияние на по-нататъшното реализиране и включване на индивида в криминалния тип дейност.

Според Douglas (1986): „профилирането е техника за идентификация на личностни и поведенчески характеристики на индивида, въз основа на анализ на това, което той/тя е извършил като престъпление“ (Douglas, 1986:405).

Маджаров (2006) го определя като важна приложна сфера на криминалната психология, която служи за разрешаването на практически задачи по профилактичната, оперативната, следствено-съдебната и пенитенциарно-пробационната дейност на различен тип личности, извършили противоправни действия. Според него то съдържа информация за индивида, която обхваща „...неговият вътрешен свят, потребностите и подбудите,

лежащи в основата на постъпките му, емоционално–волевата сфера, способностите и особеностите на интелектуалната му дейност“ (Маджаров, 2006: 31).

Ainsworth (2001) предлага няколко модела за анализ при правенето на психологически профил, а именно: анализ на местопрестъплението, диагностична оценка и прилагане на юридическа психология. Canter и Youngs в книгата си: „Investigative Psychology: Ofender Profiling and the Analysis of Criminal Action“ (Разследваща психология: профилиране на извършители и анализ на криминалните действия, 2009) правят разграничение между разследване (в частност разследваща психология), използващо профилирането като метод и статистическия подход към този тип психодиагностика.

Alison и Kebbell пък през 2006 г. обособяват два основни метода за прилагане на профил. Това са хомологичната и съгласуваната предпоставка. Втората предполага, че различните извършители биха прилагали подобно поведение при всичките си престъпления, докато при хомологичната предпоставка се смята, че „сходни престъпления би трябвало да се асоциират със сходни минали поведенчески характеристики“ (Alison and Kebbell, 2006:153).

Съотнасяйки психологическия профил към извършителите на компютърни престъпления, Kirwan, Power (2011) дават примери за двата типа предпоставки. В случая със съгласуваната предпоставка, ако е налице измама с търг на дадена стока от някой сайт, то извършителите биха действали по същият начин (със същия тип измама) и за друг тип онлайн престъпления. Ако съпоставим примера с онлайн измамата с втората предпоставка, то от значение би било как точно лицето разбира самото престъпление и как то го извършва. Може би поради факта, че то е способно да извърши такъв тип поведение в ежедневната си комуникация би било изключително предпазливо относно документи, търгове и лични файлове на собствения си компютър (Kirwan, Power, 2013:5).

Тъй като поведението е своеобразно отражение на личността, се възприема становището, че чрез възпроизвеждане и ре-

троспектиране на криминалното деяние, би могло да се даде доста точна и достоверна представа, както и интерпретация на самия извършител.

Това се отнася до всички видове престъпления, независимо дали са били офлайн. В това лежи и основата на профилирането като метод за прогнозиране. Така чрез анализ на личностната структура (подбуди, мотиви, цели, начин на живот, фантазии, взаимоотношения и други), на избора на местопрестъпление и жертва, както и на поведението на извършителя преди, по време и след самото престъпление може да се направят хипотези, като по този начин да се стесни кръга от заподозрени лица и да се стигне до истинският извършител.

От информация на ФБР (2015) психологическото профилиране помага при разследване на криминални престъпления от 76 до 93% от случаите като задачата на профила е да създаде реалистична престава за доминиращите индивидуални характеристики на неизвестния извършител с цел изграждането на надеждна оперативна версия и неговото залавяне. В контекста на личната му детерминираност социалните, биологичните, психологичните и криминалните мотиви на тези лица дават основа за интерпретиране на предприетите от извършителя действия, което определя неговата уникалност, но и служи за опорна точка при изготвянето на профила му.[1]

Оценка на престъпния акт

Обикновено това е действие насочено срещу конкретен човек. Често дори е провокирано от самия него. Извършителят го приема като вид заплаха и решава чрез противоправното деяние да го накаже като се търси показност на надмощие и власт. Така, за да бъде подходящ за профилиране, криминалният акт е необходимо да бъде насилствен или да носи потенциална заплаха за нанасяне на вреда над жертвата. В контекста на темата става

[1] http://fbi.gov/Criminal Profiling/, изт. на 20.07.2015 г.

въпрос за всички видове киберпрестъпления, тъй като макар и с различна мотивационна установка крайният ефект е винаги нанасяне на вреда – психическа, материална или дори и физическа.

Приема се, че извършителят по време на деянието има променено състояние на когнитивните способности и/или на афективното състояние. Това дава отражение върху начина на извършване на престъплението и последиците от него. Отчитат се фактори като: фантазност (особено при педофили и сексуални насилници), завист (при различен тип хакери), конфликти (главно при кибертерористични атаки), психопатологии, употреба на алкохол и наркотични вещества, междуличностни отношения (често при различен тип социални престъпления като следене, дебнене, отправяне на заплахи), ситуационни елементи и обстоятелства (особено при различен тип интелектуални и материални кражби) и други.

Специфично внимание се отделя на елементите и нивото на агресия, на вида темперамент и на стресогенните фактори. При профилирането това винаги дава отражение и служи за отключваща сила за даденото престъпно или девиантно действие.

- *Стрес*

Тъй като всеки притежава собствена индивидуалност, то и личностната предразположеност към стрес има различни параметри. Стресорът се приема за събитие или преживяване, което не може да бъде преработено рационално и което носи със себе си чувство на неудовлетвореност, несправедливост и фрустрация. Затова се отделя голямо внимание на два типа поведение, предложени от психолозите М. Фридман и Р. Роузман през 1974 г. Те биват наречени поведение „тип А“ и „тип Б“.

Първото е характерно за лица, които са с високи нива на скрита агресия и които проявяват нетърпеливост, конкурентост и съревнование при повечето ситуации. Индивидите с поведение „тип Б“ са склонни да оценяват различните кризисни събития и житейски несгоди като мотивационни фактори, които им

помагат за адаптацията им към околната среда. По този начин те активно използват психологическите си и социални ресурси за справяне със стресогенните събития, което ги прави по-адаптивни и устойчиви. Хората, предразположени към криминални деяния по-често са от първият тип. Това се дължи на неспособността им за адекватна самооценка, недобре изградена Его-идентичност, както и завишените им очаквания към околните. Към тази група спадат и повечето извършители на компютърни престъпления.

• *Агресия*

Когато се говори за девиантност едно от първите неща, които изникват в представата за това понятие, е високата агресия и агресивните отговори към дадена ситуация, личност или просто като начин на поведение. Популярно в американската общественост е обяснението на агресията като вроден инстинкт за борба и като енергия, която бива натрупана в течение на времето. Колкото повече се е натрупала, толкова по-малък стимул е необходим за нейното задействане, което води до открито агресивно поведение.

Ако е изминало достатъчно време от последния ѝ изблик, то откритата агресия може да се появи спонтанно без видим задействащ фактор като основната цел е да бъде изразена.

Л. Бъркович (1962) смята, че стимули, които са редовно асоциирани с агресията могат постепенно да придобият способността да предизвикат агресивни действия в предварително провокирани хора. Според него фрустрацията бива предизвикана от гняв, който сам по себе си не води до открита агресивност, а само до готовност и нагласа да се реагира враждебно в даден момент.

Той постулира, че за да се прояви открита агресия трябва да има подходящи релевантни знаци като хора, места или различни предмети, които са свързани с настоящи или отминали провокатори на гняв (Berkowitz, 1962). За извършителите на компютърни престъпления такива могат да бъдат дори качването на

определена информация, особено в социалните мрежи, която да служи за стресогенен фактор от страна на самият извършител и да провокира в него такъв тип действие.

Според Е. Арансън (2009) обикновено има три начина за освобождаване на агресивността.[1] Последният е чрез непосредствена агресия – когато личността се нахвърли върху човека, който е причинил раздразнението ѝ, искайки и успявайки да го нарани, да му причини неприятности, да злослови по негов адрес и други прояви, обикновено свързани с асоциално и девиантно поведение (Арансън, 2009). Съотнасяйки последния пример към компютърните престъпници, голяма част от тях извършват атаките си главно за да обидят, наранят или оскърбят дадена личност с цел задоволяване на собствените си нужди от признателност, контрол и подчинение на околните.

Използвайки този тип агресивни методи компютърът се явява само медиатор на действията им като от основно значение е ценностната нагласа и готовността за определен тип отреагиране. Косвената агресия е доста характерен пример за това. При нея агресивните действия са плод на въздействието на друг индивид или група хора върху поведението на агресора. Индиректните въздействия включват манипулативни послания, заплахи или демонстрации. Киберпрестъпниците главно поради естеството на престъпленията и това, че няма реализиран физически контакт осъществяват различен тип косвена агресия, която може да варира по отношение на интензивността си.

Друг тип агресивност, използвана при осъществяването на компютърни престъпления е инструменталната. Тя е вид инструмент, чрез който личността удовлетворява свои потребности или постига поставените си предварително цели. За разлика от вербалната, включваща различен тип обиди, заплахи и нега-

[1] Първият е като се изразходва агресивността под формата на физически упражнения (игри, бягане, скачане, боксиране и други). Вторият е като се насочи към неразрушителна форма на въображаема агресия – например когато индивида си представя как удря някого или пише разказ, пълен с актове на насилие.

тивни оценки, главно чрез анализ на чуждото поведение, при инструменталния тип агресорът предварително знае какво иска да постигне и прибягва до похвати, които са му познати.

Освен собствените си действия, той може да използва като инструмент и психологическите нагласи на другите хора с цел да ги манипулира за постигане на собствени желания, амбиции и цели.

• *Агресивно поведение*

В исторически план всички социални общности имат в себе си заряда на деструктивната форма на поведение, свързана със съзнателното желание на индивида за нанасяне на физическа или психическа вреда, стигаща до унищожение или самоунищожение. В психология на девиантното поведение обаче този феномен се разкрива чрез **агресивното поведение**.

Данни за неговото присъствие в обществото, независимо от опитите на различните школи за нейното обяснение, съществуват още в древността. Приоритетно е описанието на агресивните действия, които се оценяват от гледна точка на морала и нравствените ценности. То започва да се представя като структура, съдържаща в себе си агресивни нагласи, отношения, оценки и агресивни действия, като се търси връзката между тях.

Изхожда се от факта, че трябва да се разграничават две основни понятия – агресия и агресивно поведение. При компютърните престъпници последното може да бъде провокирано от различен тип фактори като:

- Установени смущения в социализацията на личността, водещи до промяна на нагласи, цели, мотиви, ценности, убеждения и емоции. Това може да се наблюдава при всички видове, но е особено изразено при педофилите, сексуалните насилници и разпространителите на порнография.
- Привикване на отделната личност към стереотипа на поведение, имащо в основата си противообществен характер, т.е. демонстрацията на агресивни механизми води до включване в поведението на т.нар. агресивни стереотипи като поведенчески актове, ориентирани към използването на агресия

и антисоциални изяви в различни ситуации. Например при различен тип кражби и измами било то чрез използването на компютърни технологии или на традиционните методи на извършване.

- Агресивното поведение се разглежда като стереотипно, но носещо в себе си силно емоционално напрежение. Лицата, които го прилагат имат висока тревожност, нисък праг на търпимост, затруднения в оценяване на актуалната ситуация, както и стремеж за доминиране в нея, проява на упоритост и липса на отстъпчивост. Често при кибершпионаж, следене, тормоз, неправомерно проникване и разпространение на данни, в оценката за възприемането на другия човек се включват критерии, които не се отнасят до неговите личностни характеристики, а до оценката на неговите действия като враждебни. Стереотипността предполага и невъзможността друг вариант на поведение да се окаже актуален, т.е. установява се разминаване между собствените оценки и оценките на другите хора, което води до преживяване на безсилие и безпомощност от страна на извършителя. За избягването на тези чувства се предприема действие, което да намали техния интензитет.
- Проявата на агресивност води до ограничаване на социалните интеракции. Често такъв тип индивиди живеят много повече във виртуалния свят, със своят виртуален Аз, приятели и поведение, отколкото в реалния, което води до ограничаване на реалните социални контакти или тяхното избягване. Това може да доведе до чувство на неудовлетвореност от общуването с околните и тяхното възприемане като противници, а оттам и желанието за победа и/или конфронтация с тях.

Обобщено може да се твърди, че когато в поведението е налице агресия и когато тя е активна, то самоконтролът бива намален, т.е. колкото по-висока е агресивността, толкова по-нисък е самоконтрола. Оттам действията на индивида стават реактивни и той предпочита преустановяване на взаимодействието си с околните. Така агресивните действия, съпроводени с антисоциални прояви, особено когато се прилагат активно, променят

психологическите характеристики на личността, като я подтикват да бъде неотстъпчива, злонамерена, злопаметна, трудно да извършва логически ситуативни връзки и често от страха си за неуспех да прилага жестокост.

• *Темперамент*

Разликите в поведенческите стереотипи и цялостния характер на отделните лица – техните предпочитания, нагласи, потребности и мотиви могат да бъдат обяснени с термина темперамент. Започвайки от Хипократ и стигайки до Кречмер, Юнг и много други, търсенето на онази част, която би могла да обясни поведението, респективно характера на даден индивид продължава и до днес.

Изследвайки и анализирайки го, се стига до възгледа, че много от извършителите на различен тип девиантни, също така и делинквентни прояви притежават характерни черти, които ги отличават от останалата популация. Избухливост, затвореност, изолация, неуравновесеност, слабо изградена Аз-концепция с високи нива на егоцентризъм, агресия, напрежение и емоционална лабилност, но и слабост са характерни черти за различен тип извършители на киберпрестъпления, главно измамници и лица, осъществяващи психологически атаки върху жертвите си като следене, заплахи, дебнене, тормоз или разпространение на порнографски материали.

Оценка на местопрестъплението

Мястото на извършване на престъплението винаги оставя след себе си определена информация, която служи за по-прецизното профилиране на неизвестния извършител.

От оценката на престъпния акт се съди главно за психическото състояние на лицето, докато от тази на местопрестъплението могат да се разберат неговите отличителни характеристи-

ки като начин на действие, почерк, евентуалната инсценировка и дали са били взети сувенири и трофеи.[1]

• *Начин на действие*

Начинът на действие или modus operandi е поведение с висока доза на планомерност, организираност и целенасоченост на действията. Той показва всички онези поведенчески актове, които извършителят е предприел за осъществяване на деянието.

Това е вид заучено поведение, което остава константно във времето като по този начин гарантира сигурността на извършителя, предпазвайки неговата самоличност и улеснявайки го при реализацията на престъплението. [2] Изменения в него биха могли да настъпят следствие реакциите на жертвата, както и от опита на самия деец или ако има сериозна опасност за неговата идентификация.

• *Почерк*

Ако modus operandi показва действията, то почеркът (signature) се фокусира върху самото поведение. Това понятие е въведено от експертите по профилиране на ФБР, за да покажат ритуалните действия, включващи фантазен елемент по време на извършване на престъплението, т.е. поставя се акцент върху детайлите, които помагат за разкриване на особеностите на извършителя. И ако начинът на действие (дори и рядко) би могъл да бъде изменен, то почеркът е независим от обстоятелствата и причините, които биха могли да променят действията на дееца. Това показва, че е различен и не съвпада с начина на извършване на престъплението.

---

[1] Последните две са особено характерни за извършителите на убийства и на насилствени престъпления.

[2] Както при отделните форми на престъпност, така и при киберпрестъпленията това дава основна информация за извършителя, помагайки по този начин да бъде идентифициран. Тези начини ще бъдат представени в рамките на настоящата книга.

Тъй като е продукт на фантазиите и въображението на лицето, той винаги издава аспекти от личността му, развивайки и засилвайки се с всяко следващо деяние като проявата му не на всяка цена бива изразена, поради осуетяване или неблагоприятни ситуации.

Website defacement (deface) е един от основните видове почерк, главно при хакери. Това се изразява в оставяне на определено послание или вид подпис на извършителя в системата на потърпевшото лице.

• *Инсценировка*

Често при различен тип престъпления се използва и инсценировка. Това е умишлено изменение в обстановката на местопрестъплението, целящо да осуети разследващите органи и да ги насочи към погрешен извършител или насока. Към това може да се причисли всяко едно физическо изменение на мястото, предметите или на жертвата.

Съотнасяйки инсценировката към киберпрестъпленията, тъй като няма физически контакт нито с жертвата, нито със самото място, което е виртуално, то би могло в нея да се причислят инперсонализацията на чужд акаунт, от който се извършва действието.

• *Трофеи и сувенири*

Трофеите и сувенирите също са включени в изготвянето на профила за оценката на мястото на извършване. Разликата между двете е, че трофеите са вещи, взети от мястото, които не притежават особена реална ценност (тя е по-скоро психологическа и служи за самоутвърждаване, завладяване и победа над жертвата), те биха могли да бъдат изхвърлени след известно време от престъпника, а сувенирите са вещи от самата жертва, като целта им е да бъдат запазени.

По този начин се преживява отново и отново победата и чувството на контрол и доминация над нея, връщайки мислов-

но дееца към момента на извършване на престъплението и преживявайки усещанията, по време на неговото осъществяване. В случая с извършителите на компютърни престъпления примерни за това могат да бъдат специфичен тип лична информация като снимки, документи и отделни данни за жертвата, които са били откраднати.

Оценка на жертвата

Доста често при изготвянето на профил се установява, че извършителят е познавал жертвата. Ако не лично, то поне е запознат с нейния профил и история, или с информацията споделена за него във виртуалното пространство. Това поставя въпроса доколко тя спомага или предизвиква нападателя си.

Става въпрос за ситуационните елементи и обстоятелства преди извършването на престъпление. Тези елементи образуват контекст, който акцентира на близки отношения между двата субекта (извършител – жертва). Той е и причината за мотивацията на криминалния акт, която обикновено бива два вида – инструментална и експресивна.

Първата представлява планирано умишлен акт за постигане на дадена цел, често материални средства или заемане на по-висок статус в обществото. Престъпленията свързани с измами и кражби на финансови средства, кибертероризъм, и различен тип хакерски атаки се извършват главно от такъв тип мотивация.

Експресивната мотивация е непланирано действие, в много случаи осъществено спонтанно, при което са налице гняв, ярост или обида. В доста голям процент от престъпления като кибер-следене, шпионаж, тормоз, манипулация с информацията от социалните мрежи те са продиктувани от такъв тип действия, т.е. от определен вид поведение на самата жертва към извършителя.

При ситуационните обстоятелства от значение са: средата на жертвата, познанствата ѝ, интересите и навиците, както и местата, които посещава.

• *Виктимология*

Съществуват три типа потенциални жертви – ниско, умерено и високо рискови, в зависимост от поведението, индивидуалните им качества, както и от социалния и професионален статус.

Най-застрашени от криминални посегателства са умерено и високорисковите. Техният начин на живот ги поставя в ситуации на висока застрашеност, като последните често биват виктимизирани (или подпомагащи виктимологията).

В голяма част от случаите на киберпрестъпления, главно на шпионаж, тормоз, както и на различен тип хакерски атаки самата жертва е помогнала по пряк или косвен начин извършването на определен вид престъпление върху нея – било то чрез споделяне на прекалено много лична информация или на демонстриране на поведение, смятано за провокативно от страна на извършителите.

Така представено от оценката на жертвата изглежда, че тя има важна роля в процеса на протичането на престъпния акт, като с действията или бездействията си може да се окаже пряк регулатор на поведението на неизвестния извършител, което да помогне за изготвяне на първоначалните хипотези относно мотивите му.

Виктимологията показва хистероидната акцентуализация и нива на висок риск при определен тип поведение главно от страна на нежният пол. Това се изразява в тип демонстративно държание, афиширане на лични взаимоотношения, привличане на вниманието на околните върху себе си било то чрез материални средства или чрез определено положение и контакти в личната или професионална сфера. Това са т.нар. високо рискови жертви, чийто начин на живот ги виктимизира като постоянно ги излага на криминогенни фактори.

Друг тип лица, ставащи жертви на компютърна престъпност от този тип са умерено рисковите жертви. Те „рядко са с добра обществена репутация и с поведението си създават нарастващи възможности да станат криминални жертви – прибират се късно вечер или рано сутрин, посещават съмнителни заведения...“.