The empirical investigation of the discovery of the attitude to the secure educational environment and the measuring of teenagers tendency to the realization of different forms of victims behavior. 32 students of comprehensive secondary school: among them: 20 students of the 9th form, 12 – of the 8th form at the age of 13–15 took part in the investigation.

In the course of analysis of the results achieved from the questionnaire "The appearance of victimiology in behaviour" displaysthe fact that 25 per cent of students are victims. The main behavioral characteristics are infantilism, demonstrativism, the fear of responsibility, externality, manipulation by people. The social role of a victim was revealed among 50 per cent of pupils. This fact says that such pupils possess the feeling of being a social outcast, the surrounding world seems hostile to them. The position of a victim is determined among 19 per cent of pupils.

All the characteristics of the game role of the victim are preserved, they get an expressive character. They are such characteristics as infantilism, the fear of responsibility, externality. The status of a victim is revealed among 6 per cent of pupils.

This fact says about embodiment of the social role of the victim, about strong education, which includes total combination of rent directives. They are consolidated in pupil's model of behavior by effort of main characteristics of a social role and contribute to person's deformation in his behavior.

In the course of analysis of the results from the questionnaire "Psychological diagnostics of educational environment security of school" for pupils the following fact was achieved: the pupils with manifestation of factious victim role, the position of a victim consider the educational environment more secure than pupils with manifestation of social role of a victim and the status of a victim.

According to mentioned ideas we may come to the conclusion that one of the main tasks of social-pedagogical service at school is the control of psychological and physical health of all the participants of educational process. Besides, among students there is a necessity of formation of the system of knowledge, skills of secure behavior in difficult life situations and rendering assistance while looking for constructive ways out from them.

REFERENCES

1. Стреленко, А.А. Социально-перцептивные образы виктимной личности : моногр. / А.А. Стреленко. – Витебск : УО "ВГУ им. П.М. Машерова", 2009. – 138 с.
2. Баева, И.А. Психологическая безопасность в образовании : моног. / И.А. Баева. – СПб. : СОЮЗ, 2002. – 271 с.
3. Христенко, В.Е. Психология поведения жертвы / В.Е. Христенко. – Ростов-н/Д : Феникс, 2004. – 298 с.
4. Клейберг, Ю. Психология девиантного поведения / Ю. Клейберг. – М. :Творческий центр, 2001. – 298 с.

UDC 347.66

THEORETICAL AND PRACTICAL PECULIARITIES OF THE INSTITUTE OF DIGITAL INHERITANCE

KRYSTSINA SAVITSKAYA, VLADIMIR BAHANENKA
Polotsk State University, Belarus

The work is a comparative analysis of theoretical and practical peculiarities of the Institute of digital inheritance. The analysis of the current legislation in the sphere of digital inheritance has been carried out. The terms of Service of different Internet providers have been studied. The issue of the correlation of the Terms of Service of different Internet providers and current legislation in this area has been considered. In the final part we have drawn the conclusion about the features of the Institute of Digital inheritance and have made development prospects.

People have been transitioning remnants of their identity from conventional physical effects, such as photos and trinkets, to online profiles and social networks. Identity is being digitalized, this raises certain difficulties such as the population ages [1]. A significant portion of modern decedent's assets may consist of digital assets' such as e-books, domain names, and online accounts. Unlike their tangible predecessors, digital assets may be difficult for executors and administrators to obtain. Death today presents more complex issues than before the digital age. As far as death questions are concerned, components of online identity do not fit the mold of the traditional framework of the society.

With the ever-increasing landscape of online accounts, social networking websites, and web-based email accounts, it has become more and more common for people to have numerous online accounts with different usernames and passwords. This creates an issue for estate planners in terms of what will happen to these accounts and the personal information stored in them after a person's death. One of the first problems facing estate planners is that there is currently no proper definition of a digital asset or a digital estate provided in either Dictionary or Law Dictionary. With no definition to act as a compass, estate planners are left guessing as to what will qualify as a digital asset.

Before pressing on into how digital assets and estates should be planned for, a working definition must first be established. Currently, no definition exists, which proves to be a challenge to estate planners. A proper definition, however, would not only provide practicing estate planners with a proper compass, but it would also serve to allow estate planners, courts, and other practicing attorneys to be able to identify digital assets and to decide what amount of legal protection the assets should receive [2] .

Nathan Dosch, an estate planning and tax attorney with Neider& Boucher and creator of the Digital Estate Planning Blog, pieced together definitions of "digital" and "asset" from Webster's Dictionary in order to define digital asset as "any file on your computer in a storage drive or website and any online account or membership". Examples of digital assets include documents created via a Microsoft Office Program (e.g. Word, Excel, or PowerPoint), digital photos, digital videos, music on iTunes [3].

Additionally, digital assets include online accounts and memberships such as e-mail accounts, profiles on social networking sites such as Facebook and MySpace, online digital photo accounts, online banking and credit card accounts, and websites or domain names owned by a person, and any online subscription accounts.

Additionally, digital assets and estate might be considered "virtual property" (note that virtual property and digital assets are one and the same), which would include things such as "a website, a bidding agent, a video game character, or any number of other intangible, digital commodities" [2]. Therefore, the working and suggested definition of a digital asset for this comment will be: any digital file on a person's computer as well as online accounts and memberships [4].

While this definition might seem broad, it should be noted that a broad definition is necessary in order to encompass everything that is in fact a digital asset. Therefore, digital assets must not only include those documents that a person creates (via Microsoft Word, Excel, or PowerPoint), but it must also include all owned domain names, any legally downloaded files (e.g. MP3 Music Files and Movies), and any web-based personal accounts that require a username and password for access (e.g. a social networking account, a web-based e-mail account, and any accounts storing personal information; such as online banking account sand online shopping accounts).

Digital assets, therefore, can be found in many different forms. For example, some digital assets may be stored on a computer or smartphone or uploaded to a website. These assets would include items such as music, videos, medical records, tax documents, financial records, photographs stored on websites such as Shutterfl y or Flickr, or generic file storage sites in the Cloud such as Dropbox. Most, if not all, of these types of digital assets require a login ID and password to gain access to the stored materials.

Other assets involve social media websites, such as Facebook, LinkedIn, Twitter, Pinterest, or Google Plus etc, which promote social interaction, messaging and connection to other individuals.Many of these sites also offer storage for photographs and videos. Again, these types of digital accounts typically require a login ID and password to gain access. In addition, there are many other types of accounts that we use in our daily lives that have secured access. These accounts include email accounts such as Yahoo!, Gmail or Hotmail, It should be noted that these email account providers are free services. Many people pay a fee for their email service to companies such as Time Warner Cable, Optimum Online and AT&T. For these types of services, the email accounts will remain active as long as the fee is paid. These accounts also comprise on-line banking accounts, Paypal accounts, eBay accounts and Amazon accounts, just to name a few. Certain digital assets have their own pecuniary value such as ownership of a domain name or a blog. It is no wonder that with all of these digital assets, estate planners and administrators are wondering how to deal with them after the death or incapacitation of the "owner" [5].

In own research Naomi R. Cahn separates different categories of digital assets: personal, social media, financial, and business [6].

Although there is some overlap, of course, clients may need to make different plans for each. An inventory of each of these assets should include the domain name, user name, and password, and, when known, the date the account was created.

It is also important to determine what definition of property that digital assets will fall into. Generally, property is divided into two types: real and personal. On the one hand you have real property, which is essentially land and anything that is attached to it **[**3]. Personal property, on the other hand, is anything that is not

real property. Additionally, personal property is further divided into two subcategories, "tangible (car, furniture, jewelry, art, clothing, appliances) and intangible (stocks, bonds, patents, trademarks, copyrights)" [3]. This distinction is important because digital assets have the unique potential to change from an intangible asset to a tangible one. A digital asset, such as a digital photo or e-mail, can change from intangible property to tangible property simply by printing out a copy of it. Whether an item of personal property is classified as intangible or tangible has the potential to completely alter the probate process.

Therefore, unless a proper definition is established and decided upon, estate planners will continue to have issues not only deciding what exactly will qualify as a digital asset, but they will also face substantial issues regarding how to properly prepare for what will happen client's digital assets and estates after their death.

Digital assets are not the first intangible assets that estate planning attorneys have faced. Copyrights, for example, are capable of probate and non-probate transfer. But copyrights clearly belong to the holder rather than being subject to terms of service with another party. If the analogy is instead to tangible assets, such as bank accounts, then few problems should arise when the executor or personal representative seeks to collect estate assets.

Nonetheless, few states have laws directly on point, and few court cases address these issues. One of the only such cases involved Justin Ellsworth, a soldier killed in Iraq, whose father wanted access to his son's Yahoo! e-mail account. When Yahoo refused to provide access, the father went to court, and a probate judge ordered Yahoo to turn over the e-mails [7]. Even in this situation, Yahoo was not required to provide access to the actual account.

Connecticut has enacted legislation that responds to situations like that involving Cpl. Ellsworth and requires e-mail providers to turn over copies of all e-mails (sent and received) to the executor or administrator of a decedent's estate. Conn. Gen. Stat. § 45a-334a [6]. The legislation does not cover other on-line accounts, however, and it is unclear whether a testator could prevent this result or require the provider to transmit the e-mails to another individual [6].

Indiana explicitly requires "any person who electronically stores the documents or information of another person" to "provide to the personal representative of the estate of a deceased person, who was domiciled in Indiana at the time of the person's death, access to or copies of any documents or information of the deceased person stored electronically by the custodian." Ind. Code § 29-1-13-1.1 [6].

Oklahoma has enacted an even more comprehensive statute. The law, which became effective on November 1, 2010, states: The executor or administrator of an estate shall have the power, where otherwise authorized, to take control of, conduct, continue, or terminate any accounts of a deceased person on any social networking website, any microblogging or short message service website or any e-mail service websites. 58 Okla. Stat. Ann. § 269 [6].This statute is a start but, by its own terms, does not authorize full-blown access to all of the decedent's digital property. First, it is limited to the sites that are covered. Second, it explicitly grants the executor power only "where otherwise authorized". A general problem is that on-line sites can claim the ability to control the transfer of accounts through their user agreements, and these service agreements can contain terms that, arguably, would not permit the ac-counts to survive the decedent or allow anyone else, even an executor, to access the accounts. Consequently, service providers might challenge any effort to apply the law when it allegedly violates a service agreement. They might also claim not to be controlled by Oklahoma law. On the other hand, analogizing on-line content to laws applicable to bailment, safe deposit boxes, and more traditional types of probate assets might be productive in recognizing the rights of an executor to the on-line property of the deceased [8].

Few states have enacted statutes to deal with electronic content and digital assets. That means for most people in most states, if the service provider has a policy regarding the transfer or disposal of account access and content under the provider's Terms of Service ("TOS"), then the TOS will control the fate of the deceased person's account and content for that service provider. Service providers routinely amend the TOS agreements with no notice to the account holder, so it is wise to periodically check the service provider's website for any changes to the TOS. Most people agree to the TOS of the service provider by clicking on the "I agree" button when establishing an account [6]. Some service providers have a policy that indicates what will happen upon the death of an account holder. Others have no detailed policy. For example, Shutterfly's TOS does not include an explicit discussion of what happens when the account holder dies. Shutterfly's TOS states that the individual agrees not to disclose his or her username or password to any third party and acknowledges that the individual's access to the account is non-transferable [9].

The TOS for Linked In, Google and Twitter each contain similar language regarding disclosure of the secured access information and transferability [10; 11; 12]. Conversely, Gmail has a policy for potentially releasing emails to the personal representative of a deceased account holder [13].

The policy makes it clear, however, that there is no guarantee the email content will be released and a court order will be required [13].

Yahoo! explicitly states in its TOS that the account can not be transferred and any rights to content within the user's email account terminate upon death and all content may be permanently deleted [14]. Facebook allows someone to report a user as deceased and the deceased user's Facebook page may then be converted into a memorial to the deceased user. Only confirmed friends will continue to have access to the deceased user's profile and may continue to post messages in memoriam on the deceased user's wall [15].

A more complex issue surrounds the choice of law clause that is generally included in a service provider's TOS.

A choice of law clause dictates which state's law will govern the TOS itself and any transaction that is related to the TOS. The result may be that even where the deceased resides in a state with a statute governing the disposition of and access to the deceased's digital assets, if the state law governing the TOS does not have a similar statute, the TOS may override the state law where the deceased resides. Current Law Regarding Fiduciary Access to Digital Assets At the time of this writing, only six states, Connecticut, Rhode Island, Indiana, Oklahoma, Idaho, and Virginia, have enacted statutes to deal with electronic content and digital assets. These statutes make good progress towards resolving the digital asset dilemma. However, the Oklahoma and Idaho statutes do not authorize full-blown access to all of the decedent's digital property. In addition, the Oklahoma statute expressly grants the executor power only "where otherwise authorized" [16]. This language can give the service provider the ability to claim control over the transfer of the deceased's account through the TOS. As discussed above, most service providers utilize a TOS that does not allow for transfer or assignment, much less access to the deceased's accounts by a fiduciary. Finally, Virginia's statute was very recently passed in March 2013, and was crafted to specifically address the inability of the parents of the 15-year old who committed suicide to gain access to their son's Facebook account [16]. The statute, however, appears to only address the access of digital accounts that were controlled by a minor.

In this research, we have outlined the central challenges relating to what happens to digital artifacts after users die. It should be noted that currently there is no single model of inheritance and wills digital assets. This failure to engage with user death impacts adversely on both users and industry. To solve this problem it is necessary to find a balance between the interests of the privacy policy and the internet- providers need access to digital assets of the deceased heirs and executors of the will. As the Internet continues to grow and expand, so does the need for estate planners who are able to assist their clients in ensuring that the client's digital assets and estate are properly planned. Unfortunately, however, despite the increasing popularity of web-based accounts there has still been little to no legislation regarding this area of estate planning.

REFERENCES

1. Mauer, J. Research Note Risks in Digital Identity After Death [Electronic resource] / J. Mauer. – 2013. – Mode of access: http://anniesearle.com/web-services/Documents/ResearchNotes/ASA_Research_Note_RisksinDigitalIdentityAfterDeath _July2013.pdf. – Date of access: 20.12.2013.
2. The Five Indicia of Virtual Property, 5 PIERCE L. REV. 137 (discussing the "five indicia" for determining what is a legally protectable digital asset). [Electronic resource]. – 2006. – Mode of access: http://law.unh.edu/assets/images/uploads/publications/pierce-law-review-vol05-no1-blazer_1.pdf. – Date of access: 20.06.2014.
3. Dosch, N. Over View of Digital Assets: Defining Digital Assets for the Legal Community [Electronic resource] / N. Dosch. – 2010. – Mode of access: http://www.digitalestateplanning.com/. – Date of access: 20.06.2014.
4. Conner, J. Digital Life After Death: The Issue of Planning for a Person's Digital Assets After Death [Electronic resource] / J. Conner // Est. Plan. &Cmty. Prop. LJ. – 2010. – V. 3. – P. 301. – Mode of access: http://heinonline.org/HOL/LandingPage?handle=hein.journals/epcplj3&div=18&id=&page=. – Date of access: 20.06.2014.
5. Beier, J.C. The Digital Asset Dilemma [Electronic resource] / J.C. Beier, S. Porter. – 2013. – Mode of access: http://www.mcglawyer.com/pdf_files/TrustsandEstatesSummer2013.pdf.
6. Cahn, N. Postmortem Life On-line [Electronic resource] / N. Cahn // Prob. & Prop. – 2011. – V. 25.– P. 36. – Mode of access: http://heinonline.org/HOL/LandingPage?handle=hein.journals/probpro25&div=39&id=&page=. – Date of access: 20.06.2014.
7. Chambers, J. Family Gets GI's E-Mail [Electronic resource] / J. Chambers // Detroit News. – 2005. – Apr. 21. – P. 1. – 2005. – Mode of access: www.justinellsworth.net/email/detnewsapr.htm. – Date of access: 20.06.2014.
8. Darrow, J.J. Email Is Forever... Or Is It? [Electronic resource] / J.J. Darrow, G.R. Ferrera // J. Internet L. No. – 2008. – V. 11.– C. 10, 1, 18. – 2008. – Mode of access: http://www.digitalestateplanning.com/. – Date of access: 15.07.2014.
9. Annual Print Plans – Terms and Conditions [Electronic resource]. – 2014. – Mode of access: http://www.shutterfly.com/help/terms.jsp. – Date of access: 08.08.2014.

10. Пользовательское соглашение LinkedIn [Electronic resource]. – 2014. – Mode of access: http://www.linkedin.com/static?key=user_agreement&trk=hb_ft_userag. – Date of access: 08.08.2014.
11. Google Terms of Service [Electronic resource]. – 2013. – Mode of access: http://www.google.com/intl/en/policies/terms/. – Date of access: 08.08.2014.
12. Twitter Terms of Service [Electronic resource]. – 2013. – Mode of access: https://twitter.com/tos. – Date of access: 08.08.2014.
13. Accessing a deceased person's mail [Electronic resource]. – 2013. – Mode of access: http://support.google.com/mail/answer/14300?hl=en&ref_topic=1669055. – Date of access: 10.08.2014.
14. Yahoo policy [Electronic resource]. – 2013. – Mode of access: http://help.yahoo.com/kb/index?page=product&y=PROD_ACCT&locale=en_US. – Date of access: 10.08.2014.
15. Что происходит при установке памятного статуса для аккаунта умершего пользователя? [Electronic resource]. – 2013. – Mode of access: http://www.facebook.com/help/?ref=pf#!/help/103897939701143/?q=death&sid=0G0Ow9oru3HcT7v4v. – Date of access: 15.08.2014.
16. Tracy Sears, Family, lawmakers push for Facebook changes following son's suicide [Electronic resource]. – 2013. – Mode of access: http://wtvr.com. – Date of access: 15.08.2014.

UDC 347.77

THE MAIN TYPES OF CYBER CRIMES ON THE INTERNET

TATSIANA SIAMIONAVA
Polotsk State University, Belarus

Cyber crime is emerging as a serious threat. Worldwide governments, police departments and intelligence units have started to react. Initiatives to curb cross border cyber threats are taking shape.

Cyber crime is a term used to broadly describe criminal activity in which computers or computer networks are a tool, a target, or a place of criminal activity and include everything from electronic cracking to denial of service attacks. It is also used to include traditional crimes in which computers or networks are used to enable the illicit activity. Computer crime mainly consists of unauthorized access to computer systems data alteration, data destruction, theft of intellectual properly. Cyber crime in the context of national security may involve activism, traditional espionage, or information warfare and related activities.

Cyber Stalking

Cyber stalking is the use of the Internet or other electronic means to stalk someone. This term is used interchangeably with online harassment and online abuse. Stalking generally involves harassing or threatening behaviour that an individual engages in repeatedly, such as following a person, appearing at a person's home or place of business, making harassing phone calls, leaving written messages or objects, or vandalizing a person's property [1].

Cyber stalking is a technologically-based 'attack' on one person who has been targeted specifically for that attack for reasons of anger, revenge or control. Cyber stalking can take many forms, including:

– harassment, embarrassment and humiliation of the victim;
– emptying bank accounts or other economic control such as ruining the victim's credit;
– harassing family, friends and employers to isolate the victim.

The term can also apply to a 'traditional' stalker who uses technology to trace and locate their victim and their movements more easily (e.g. using Facebook notifications to know what party they are attending). A true cyber stalker's intent is to harm their intended victim using the anonymity and untraceable distance of technology. In many situations, the victims never discover the identity of the cyber stalkers who hurt them, despite their lives being completely upended by the perpetrator.

Hacking

Hacking is a crime, which entails cracking systems and gaining unauthorized access to the data stored in them. A case of suspected hacking of certain web portals and obtaining the residential addresses from the e-mail accounts of city residents has recently come to light [2].

Crackers are people who try to gain unauthorized access to computers. This is normally done through the use of a 'backdoor' program installed on your machine. A lot of crackers also try to gain access to resources through the use of password cracking software, which tries billions of passwords to find the correct one for accessing a computer. Obviously, a good protection from this is to change passwords regularly. In computer