

Министерство образования и науки Российской Федерации
Ярославский государственный университет им. П. Г. Демидова
Кафедра иностранных языков естественно-научных факультетов

УЧИМСЯ ГОВОРИТЬ, ПИСАТЬ И ДУМАТЬ ПО-АНГЛИЙСКИ

Практикум для магистрантов

Ярославль
ЯрГУ
2018

УДК 811.111(076)
ББК Ш143.21я73
У92

*Рекомендовано
Редакционно-издательским университетом
в качестве учебного издания. План 2018 года*

Рецензент
кафедра иностранных языков
естественно-научных факультетов ЯрГУ

Учимся говорить, писать и думать по-английски :
У92 **практикум для магистрантов** / сост. : Т. В. Шульдешова,
Д. И. Пермякова ; Яросл. гос. ун-т. им. П. Г. Демидова.
— Ярославль : ЯрГУ, 2018. — 56 с.

Данный практикум предназначен для студентов, обучающихся в магистратуре на физическом факультете по направлению «Информационная безопасность». В соответствии с названием он включает в себя текстовый и методический материал по развитию навыков говорения, письма и целенаправленного логического мышления в сфере науки. Материалом для упражнений послужили работы John Swales, Martin Bates, Tony Dudley-Evans, H.G Widdowson и статьи из EURASIP Journal on Information Security (2017).

УДК 811.111(076)
ББК Ш143.21я73

© ЯрГУ, 2018

PART I

Descriptions of how things work: purpose

Exercise 1. Fill in the necessary conjunctions and prepositions: *because, of, off, such as, or, on, either, until, if, which, of.*

A water tap is a device for turning 1)... and 2)... a flow of water. Its most important parts are a rod with a handle on the top and a washer 3) ... is fixed to the bottom of the rod. The metal parts of a water tap are usually made 4) ... brass 5) ... brass resists corrosion. The washer is made 6) ... a flexible material 7) ... rubber 8) ... plastic.

When the handle is turned the rod 9) ... rises or descends because of the spiral thread. The column descends 10) ... the washer fits firmly in its "seat". 11) ... the tap is closed, no water can flow out of the pipe.

Exercise 2. Choose the right alternative (S=sentence; subordinate clause= придаточное предложение; main clause= главное предложение).

1. The description consists of 1/2/ 8 paragraphs.
2. The first paragraph describes a tap/ explains how it works.
3. The second paragraph describes a tap/ explains how it works.
4. Each paragraph contains 1/3/4/6 sentences.
5. The first sentence (S1) is/is not a definition.
6. S2 describes the main moving parts of the tap/the main fixed parts.
7. S3 explains why brass results corrosion/why brass is used.
8. S4 explains/ does not explain why rubber is often used for a washer.
9. S5 begins with a subordinate clause/with a main clause.
10. S6 explains/does not explain why the column goes down.

Exercise 3. Write a description of how a water tap works, choosing only five of the seven sentences given in the original passage.

Cause and Effect

Actions and results

Exercise 1. Make the statements about the following actions and results, using *so that*.

Example: Rub a match against the side of a match box: what is the result?

ACTION		RESULT
A match is rubbed against the side of a match-box	and as a result with the result that	it ignites

ACTION		RESULT
The burning match is inverted	SO THAT	the flame becomes bigger
The match is held pointing upwards		smaller
The match is shaken		is extinguished
A match is dropped on the surface of water		it ... on the surface of water
A coin is dropped into the water		it...
A large object is put into the glass of water		the water ...

Exercise 2. Make statements about the following actions and resulting changes *with the result that* or *and as a result*, and the words *become (+ adjective)*, *turn (+colour)*, *change into or be converted into (+noun)*.

ACTION		RESULT
a) A plant is kept away from the light	WITH THE RESULT THAT AND AS A RESULT	it becomes pale (etiolated)
b) A plant is exposed to the light		green
c) Photographic paper _____ to the light		dark
d) Blue litmus paper is placed in the acid		red
e) Red _____ alkali		blue

ACTION	WITH THE RESULT THAT AND AS A RESULT	RESULT
f) Iron is exposed to air and water		iron oxide
g) Wood is burned		1. burning gases 2. ash and 3. charcoal
h) A solution of salt and water is evaporated		steam and salt crystals

Exercise 3. Now change the above descriptions of actions and results in the same way as the example:

Example: If a plant *is kept* away from the light, it will *become* etiolated.

ACTIONS IN SEQUENCE

Preceding, simultaneous and following events

Before	the sun appears over the horizon,	the sky begins to lighten.
As		the light increases.
After		the sun climbs up the sky.
When the sun rises,		the day begins.
The day continues		until the sun sets.

Exercise 1. Each sentence contains two events, X and Y. Read out the sentence which means:

- a) X occurs at the same time as Y (simultaneously with Y).
- b) X occurs at approximately the same time as, or soon after, Y.
- c) X precedes Y.
- d) X follows Y.
- e) Y is at the end of X.

Exercise 2. Now complete these sentences using the conjunctions: before, as, after, when, until.

- f) _____ the sun rises, the air temperature rises.

g) ____ the sun reaches the highest point in the sky, it begins to descend.

h) ____ the sun descends, the air temperature falls.

i) ____ the sun sets, it approaches the horizon.

j) ____ the sun sets, the sky becomes completely dark.

k) ____ the sun sets, the day ends.

l) The night begins ____ the sun sets.

m) The night continues ____ the sun rises.

Exercise 3. Number these events in the order in which they occur when water is heated. Give simultaneous (одновременные) actions the same number.

a) The water becomes hot.

b) The gas is lit.

c) Bubbles appear.

d) Steam appears.

e) The gas is turned on.

f) Bubbles burst.

g) Bubbles rise to the surface.

h) The water evaporates.

Exercise 4. Complete the sentences according to the example:

Example: As soon as the gas is turned on, it is lit.

(X follows Y immediately)

i) As the water evaporates,

j) As soon as the bubbles burst,

k) When the bubbles rise to the surface,

l) As soon as the gas is turned on,

m) Before the gas is lit,

n) After the water becomes hot,

o) As soon as the bubbles appear,

Exercise 5. Number these events in the order in which they occur. Give simultaneous actions the same number.

a) The water ceases boiling.

b) The flame is extinguished.

- c) The water starts to boil.
- d) The water continues boiling.
- e) The gas is turned off.
- f) The bubbles disappear.

Exercise 6. Now write a description of the cycle by joining the correct half-sentences:

When the sun radiates heat,	until they reach high land.
As soon as the water vapour forms,	rain is precipitated.
While rising,	the water flows back to the sea.
When the vapour cools,	the vapour cools.
During condensation,	it begins to rise
The clods then move towards land,	clouds are formed.
When the clouds reach high land,	it condenses.
As the temperature falls,	sea water evaporates.
On being precipitated,	the air temperature falls.
After being absorbed,	the rain is absorbed by the soil.

Exercise 7. Put the stages in the right order and then match them with the expressions on the left:

Example: First, the site is bought.

Stages in building a house

First,	the drains are dug.
Then,	the materials are bought.
Meanwhile,	the house is painted.
Subsequently,	the walls are built.
At this stage,	the site is bought.
Next,	the site is levelled.
Afterwards,	the foundations are laid.
Then,	the house is ready to live in.
Later,	the roof is made.
Eventually,	the doors and windows are put in.
Finally,	the electricity and water systems are installed.

DEFINITIONS

In making a definition we normally give:

- a) the specific concept being defined;
- b) the class to which the specific concept belongs;
- c) the specific characteristics of the concept which make it different from other members of the same class.

Exercise 1. Use the following table to write a **definition** of an amplifier.

CONCEPT	amplifier
CLASS	device
CHARACTERISTICS	makes signals bigger

An amplifier is ...

NOTICE: we can also make a **generalization** about amplifiers in the following way:

CONCEPT	CHARACTERISTICS
An amplifier	makes signals bigger.

Exercise 2. Decide whether a statement is a definition or generalization.

1. A stethoscope is an instrument for studying sound generated inside the human body.
2. Hearing aids enable deaf people to hear sounds such as normal speech.
3. A frequency changer is a machine designed to receive power at one frequency and deliver it at another frequency.
4. Food technology is concerned with the processing food.

Exercise 3. Study the following passage and identify the definitions in it.

Kinematics

Kinematics is the branch of applied mathematics that deals with the motion of bodies without considering the forces which produce such motion. When a body moves, so changing its position,

the distance it has is measured by the length of its path of motion. Distance is therefore a scalar quantity. Speed is also a scalar quantity. Speed is defined as the rate of change of distance with time. The speed of a body measured in a definite direction is known as its velocity. Consequently, velocity is a vector quantity. If there is a change in either the speed of a body or its direction of motion, then the body is subject to an acceleration. We may therefore define acceleration as the rate of change of velocity with time. When the speed of a body decreases with time the rate of decrease of speed is known as deceleration.

Exercise 4. Rewrite the following definitions as generalizations.

1. A wafer is a piece of semiconductor used in transistors.
2. White noise can be defined as acoustic waves containing a wide range of adjacent random frequencies.
3. A parasitic aerial which is not fed directly but which gains its energy by being close to a driven aerial.
4. Automatic frequency control (AFC) is a feedback circuit which controls the average radio frequency of an FM receiver.
5. A resistor is an electric component designed to introduce known resistance into a circuit.

Exercise 5. Study the following paragraph and underline the definition you find in it.

A telescope is an instrument for magnifying distant objects. It has two essential parts: **the objective** which collects light from the distant object and forms a real image, and the **eye-piece** which forms a magnified image of this image. Refracting telescopes use a curved mirror of large diameter.

Exercise 6. Which of the following pieces of information does the paragraph include?

- a function of telescopes
- main structure of telescopes
- invention of the telescope
- function of the main parts of a telescope
- some types of telescopes
- different uses of the types of telescopes

Exercise 7. Use information in the passage to complete the following definitions.

A. ... is a form of ... which uses a convex lens as the objective.

A reflecting telescope is a ... which uses a curved mirror

PART II

Application of reading strategies

SYSTEMS

Exercise 1. The passage is about systems. The examples of systems are the solar system, a factory, the heart. Now answer these questions about the three systems:

1. What parts does each system consist of?
2. Which of the systems are natural and which is man-made?
3. When designing a system, such as a factory, what must be considered apart from the individual components?

Exercise 2. Now read as much of the passage in exercise 3 as necessary in order to find:

- a) the traditional dictionary definition of the term «system»;
- b) the definition proposed by the writer.

Underline each definition when you find it.

Exercise 3. Next read the passage carefully, paragraph by paragraph, and answer the comprehension questions. These will enable you to study how the different concepts related to systems are defined. The language study questions in the margins may help you.

	<p>Not long ago the term “system” was hardly used, but the idea of system has assumed more and more importance which is reflected in the widespread use of the term. We are surrounded by ecosystems, we create and live in political and social systems, we use transport systems and indeed, the most important part of us is a vital and mysterious system, our brain, part of the central nervous</p>
¹ Is the brain a system, part of a system, or both?	<p>system¹. The word systems, however, is a problem</p>
² Why is it a problem word?	<p>word ². Although everyone knows (or thinks they know) what it means, it turns out to be surprisingly difficult to define precisely. Systems are commonly defined in the dictionary as ‘a group of objects united by some form of interaction or interdependence; an organic or organized whole such as the solar system or a new telegraph system.</p>
	<p>This definition suggests that there are differences in the kinds of systems. The solar system is a natural system, a telegraph system is designed by man. There are also hybrid systems which are combinations of natural and man-made systems – hydroelectric plants, for example, or modern dairies.</p>

Exercise 4. List the different systems mentioned which are:

- a) natural
- b) man-made
- c) hybrid

<p>The dictionary definition is a good introduction to a discussion of systems. However, it is not a sufficient explanation of a special meaning of the term. The special meaning of the term ‘systems’ emerged during and after World War II as a result of the need for building combat aircraft. In building such aircraft, designers realized that they could not simply take an existing airplane and add weapons, bomb and fuel storage space, communication and detection equipment, and protective armour. Adding such equipment at random restricted the plane’s carrying capacity, speed, maneuverability, range of flight, and other vital functions.</p>	
<p>What emerged from this realization³ was</p>	<p>³What did they realize?</p>
<p>a new method of planning and development in which designers learned that they first had to identify the purpose and performance expectations</p>	
<p>before they could develop all the parts that made up⁴ the systems as a whole – and not its parts separately – that must be planned, designed, installed, and managed. What is really significant is not how the individual components function separately but the way they interact and are integrated into the system for the purpose of achieving the goal of the system. Generalizing from this example⁵, system can be defined as deliberately designed synthetic organisms comprised of interrelated and interacting components which are employed to function in an integrated fashion to attain predetermined purposes.</p>	<p>⁴In this context <i>make up</i> means: a) form; b) invent; c) reconcile d) decide ⁵ What example?</p>

Exercise 5.

1. In what way did the need to build combat aircraft result in the new concept of systems?
2. What was new about the ‘new method’ mentioned?

3. What is important about the parts of a system?

4. Which of the systems mentioned in paragraph I does this definition exclude?

<p>The concept of systems has rapidly expanded into new areas. Its military, industrial and business applications are enormous. Systems surround us everywhere. In the home, for example, there is a system whose purpose is to produce meals. The components of the system consists of the cook, the cooking equipment, the lightning, heating, water supply, storage and disposal facilities, the food, the dishes and the cookbook. All these interact in the performances of the process which are necessary to accomplish</p>	
<p>the purpose of the system⁶. In the case of the example given, meal production, the components will interact in such processes as planning the meals, acquiring, storing, preserving and preparing food, as well as sanitation and environmental control. Systems thus have a purpose and it is the purpose which determines the components of the system and also the interrelation of the processes in which</p>	<p>⁶ What interact in the performance of processes?</p>
<p>the components engage⁷. The purpose of any system is to produce a particular outcome. Systems can have different kinds of outcomes. To go back to the same example, the outcome of a meal-production system would be edible food.</p>	<p>⁷What do the components and processes depend on?</p>

Exercise 6. This table illustrates the system described in the paragraph. Complete it with some of the specific information given.

PURPOSE	COMPONENTS	PROCESSES	OUTCOME
	storage facilities		

<p>The planning, the acquisition of the food, the sanitation, and so on, can be viewed as subsystems that make up the meal-production system. A subsystem is a part of a total system which is designed to carry out a purpose⁸ whose attainment is necessary in order to achieve the overall</p>	<p>⁸ What is designed to carry out a purpose?</p>
<p>purpose of the system⁹. Subsystems operate in an integrated fashion. In a meal-production system, planning is integrated with and influenced by food acquisition, which then interacts with storage and preservation, preparation, and the other subsystems¹⁰. The effectiveness of the system depends on how well they inter-function.</p>	<p>⁹ What is necessary in order to achieve the purpose of the whole system? ¹⁰ What interacts with storage etc.?</p>

Exercise 7. Underline the definition in the paragraph.

Exercise 8. Use information from the paragraph to complete the following table.

Concept defined	Examples of concepts	Generalization about the behavior of subsystems	Examples of behaviour	Importance of subsystem in relation to system

Exercise 9. WRITING A SUMMARY

Answer the following questions about the passage. Write your answers as complete statements so that they provide a summary of the passage.

1. How can we define the concept of ‘systems’?
2. What does a system consist of?
3. What determines the content of a system?
4. What is a subsystem?
5. In what areas does the concept of systems have applications?

THE SCOPE OF ECOLOGY

Exercise 1. The following passage contains different levels of generalizations. Answer the following questions:

1. What do plants obtain from animals?
2. How do plants depend on animals?
3. Can you think of examples of relations between animals?
4. Can you think of examples of relations between plants?

Exercise 2. The answers to the questions will provide you with a prediction of the main content of the passage.

Now choose one item from the following list and read the passage rapidly in order to obtain the relevant information.

1. The purpose of ecology.
2. The way in which ecologists consider man.
3. Ways in which animals affect each other.
4. The effects plants have on other plants.

Exercise 3. Now read the passage again paragraph by paragraph in order to answer the comprehension questions. If you have difficulty in understanding the passage, the language study questions in the margins may help you. However, you do not need to answer all the language study questions yet.

	No living creature, plant or animal, can exist in complete isolation. An animal ¹ is bound to depend on other living creatures, ultimately plants, for its food supply; it must also depend upon the activities of plants for a continued oxygen	¹ Does it refer to animals in general or to a particular animal?
--	---	---

<p>²There are two examples of <i>its</i> and one example of <i>it</i> in this sentence. Do they refer to the same thing?</p>	<p>supply for its respiration². Apart from these two basic relationships³ it may be affected directly or indirectly in countless different ways by other plants and animals around it. Other animals prey on it or compete with it for the same food; plants may provide shelter, concealment or nesting material, and so on. Similarly, the animal will produce its own effects on the surrounding plants and animals: some it may eat or destroy, for others it will provide food⁴; and through its contribution of manure it may influence the texture and fertility of the soil.</p>	<p>³Which two basic relationships have just been mentioned?</p> <p>⁴What do “some” and “others” refer to?</p>
---	---	---

Exercise 4. Complete the following table to show the levels of generality expressed in the paragraph.

Level 1	Basic relationships	Other relationships	
Level 2		↓ an animal	an animal ↓
Level 3			

<p>⁶Which process?</p> <p>⁸⁻⁹Which of the following relationships do <i>again</i> and <i>more-over</i> express?</p> <p>a consequence</p> <p>b contrast</p> <p>c addition</p>	<p>The dependence on other living things is not confined to animals⁵. Though plants manufacture their own food by photosynthesis, they are dependent on animal respiration for at least a part of the carbon dioxide which they use as raw material in this process⁶. Supplies of mineral salts which they use to build up their substance can only be maintained through the activities of fungi and bacteria breaking down the organic matter left in the soil by other living creatures⁷. Again⁸, many plants are entirely dependent on animals for pollination or for the dispersal of their seeds.</p> <p>Moreover⁹, despite the apparently peaceful relationships in plant communities, there is intense competition going on for water, nutrient salts, and above all, for light.</p>	<p>⁵Does <i>this dependence</i> refer to all the relationships mentioned in paragraph 1 or some of them?</p> <p>⁷What maintains supplies mineral salts?</p>
--	---	---

Exercise 5. Suggest a title for the paragraph.

Exercise 6. List the processes for which plants need other living things.

Exercise 7. The final sentence in the paragraph concerns:

- a) relations between plants;
- b) dependence of plants on animals;
- c) peaceful relationships in plant communities.

<p>¹¹ What are a wood and a pond examples of?</p> <p>¹² Species exist in a state of balance and equilibrium. If there is a change in one of the factors which influence the species, the state of balance may be swayed. What can we deduce as the meaning of <i>swayed</i>?</p>	<p>We see, then, that other plants and animals, through their effects both direct and indirect, form an integral part of the environment of every living organism¹⁰. In a well-defined community, such as exists in a wood, or a pond¹¹, the population of plants and animals is influenced not only by physical factors like light, temperature, or humidity, but also by the complex interrelationships between the living creatures themselves. As a result, the population of different competing species exists in a state of delicate balance easily swayed¹² by the slightest change in any factor.</p> <p>5 What kinds of factors influence a community? 6 What is the consequence of these influences?</p>	<p>¹⁰ This sentence a follows the previous paragraph, chronologically. b is in contrast to the previous paragraphs c summarizes the previous paragraphs.</p>
--	--	---

<p>¹⁵Complete these statements: Man is seen as a ... His activities ... in terms of their effects. (Notice that the verb <i>is seen</i> is not repeated in the passage).</p>	<p>Ecology thus seeks to explain these interrelationships between all the different members of a community as a whole. To the ecologist the reactions and behavior of any plant or animal are like a piece of jigsaw puzzle¹³: he must find out how it¹⁴ fits into the picture of the whole community. Man is seen in perspective as just another piece in this grand jigsaw, and his activities in terms of the effects, good or bad, that they are likely to produce on the communities and soils from which he derives his food¹⁵.</p> <p>7. In what ways are living things like pieces of a jigsaw puzzle?</p>	<p>¹³For the ecologist what forms the pieces of a jigsaw puzzle? What is the whole puzzle? ¹⁴What must the ecologist fit into the picture of the whole community?</p>
--	---	--

	<p>The whole complex of the plants and animals forming a community, together with all the interacting physical factors of the environment, really forms a single unit, which has been called an ecosystem¹⁶. It will be seen that the final aim of ecology – the complete understanding of ecosystems – is an ideal one can scarcely hope to attain¹⁷. It is nevertheless an ideal well worth pursuing and valuable progress has been made towards it.</p>	<p>¹⁶What does an ecosystem consist of?</p> <p>¹⁷What is the final aim of ecology?</p>
--	--	--

Exercise 8. According to this paragraph, the aim of ecology is:

- a) realistic and valuable
- b) idealistic and a waste of time
- c) idealistic but valuable.

Exercise 9. WRITING A SUMMARY

A. Order the following statements from the passage according to their level of generality.

- a) Plants need animal respiration for the manufacture of food.
- b) Animals depend on plants and other animals in many ways.
- c) Living creatures cannot exist in complete isolation.
- d) Plants depend on other plants and on animals.
- e) Other plants and animals form part of the environment of every living organism.
- f) Animals depend on plants for their food supply.

B. Now write the statements in the form of a paragraph beginning with the most general. Use each of the following connectors once: *in addition, for example, similarly.*

PART II

APPLICATION OF READING STRATEGIES TO INFORMATION SECURITY TEXTS

A NEW APPROACH FOR MANAGING ANDROID PERMISSIONS: LEARNING USERS' PREFERENCES

1. A. From the list below choose one word or a phrase (connective elements) which could be logically used in place of the dots.

***FINALLY; THUS; AS A RESULT; TODAY; HOWEVER;
IF; ON AVERAGE***

B. Translate the abstract.

C. 1) What parts does the abstract of the article consist of (mind the meaning of connective elements)?

2) Could you imagine how these parts might be revealed in the article?

ABSTRACT

(...), permissions management solutions on mobile devices employ Identity Based Access Control (IBAC) models. (...) this approach was suitable when people had only a few games (like Snake or Tetris) installed on their mobile phones, the current situation is different. A survey from Google in 2013 showed that, (...), French users have installed 2 applications on their Android smartphones. (...), these users must manage hundreds of permissions to protect their privacy. Scalability of IBAC is a well-known issue and many more advanced access control models have introduced abstractions to cope with this problem. (...), such models are more complex to handle by non-technical users. (...), we present a permission management system for Android devices that (1) learns users' advanced features to manage these high-level rules. Our learning algorithm is compared to two other well-known approaches to show its efficiency. (...), we prove this whole approach is more efficient than current permission management system by comparing it to Privacy Guard Manager.

KEY WORDS: Android permission, Access control model, Recommender system.

1. Read the article, discuss the following questions in groups:

1. Is there a Russian equivalent of the word privacy?
2. Could you give the definition of privacy?
3. What sides of life does it traditionally include?
4. Why is the idea of privacy a dynamic notion?
5. What risk for privacy does the installation of applications on smartphones imply?
6. Have you got applications installed on your smartphone which can directly harm your privacy?
7. What does the ideal permission management mean?
8. What is the advantage of Kapuer over other approaches?

1. Introduction

I. Defining privacy and thus protection of privacy is difficult. If at the end of the nineteenth century privacy was “The right to be let alone”¹, it is hard to isolate yourself in our digitalized world that has been created to facilitate the flow of information. Some people even wonder if privacy still exists arguing that our digital life is either shared or public. Many researchers have taken a more balanced view and propose solutions to control the collection, analysis, and dissemination of personal information², as well as solution to avoid intrusion/decisional interference³.

II. Smartphones have a predominant place in this digital world. These devices being more and more powerful, they include more and more applications. A survey from Google in 2013 shows that French people have installed an average of 32.7 applications on their smartphone; most of which are free. We performed an analysis⁴ of the 50 most downloaded free applications on the Google play Store. This study showed that an Android application requests an average of 11.4 permissions, 5.72 of which can directly harm privacy⁵. Multiplying it by the number of applications per device results in a total of 372.7 permissions and 184 of which are highly dangerous to manage on each device. Each of these dangerous permissions shall be carefully chosen since some applications, not considered as trojan, collect and sell users` data under the guise of providing some services⁶. For instance, Yo³ is a free application whose unique feature

is sending a notification with word “Yo” and the current location to user’s friends. Yo requests a lot of permissions. Access to the contact list and the location seems coherent. However, Yo also asks to have access to the identity information⁷, the files, the pictures, and the camera. The privacy policy⁸ of Yo states that the company collects personal and activity data⁹, shares them with companies they trust, and keeps all these data indefinitely.

III. On Android, controlling access to applications¹⁰ is complex. Until version 5.x (included), installing an application is equivalent of granting all the permissions¹¹ requested by the application. Permission management¹² is very limited: either you authorize everything or you cancel the installation¹³. Additional permission management systems (such as Privacy Guard Manager, Permission Master, XPrivacy, or DonkeyGuard) can be installed to enhance the basic native Android system¹⁴ by allowing users to modify permissions after the installation of applications. All these permission management applications follow an Identity-Based Access Control model¹⁵, i.e., the user has to control every permission for every installed application.

IV. The ideal permission management should allow users to write high-level permissions without narrowing the capability of access control. High-level permissions will reduce the number of permissions and make the global policy more understandable. However, writing high-level policies being more complex, non-technical users would not be able to do it without help. In this article, we present a recommender-based system¹⁶, called Kapuer (KAPUER is an Assistant¹⁷ for Protection of Users pERsonal infoRmation), that assists people in managing permissions on their Android device. Kapuer includes a novel learning algorithm, based on an aggregation operator¹⁸ called Kagop (Kapuer AGgregation OPerator), to capture users’ preferences in terms of privacy¹⁹.

V. This article summarizes all our previous works on Kapuer. We proved the benefit of recommender-based systems for writing policies. We introduced a first version of our problem-solving model as well as the initial Android prototype. We described the final Android implementation²⁰. This article extends and presents the whole learning process. For the first time, we detail the latest version of our

aggregation operator Kagop, which is the cornerstone of our learning algorithm²¹. We also describe the integration of Kagop in Kapuer. And finally, we prove Kagop has better results than two well-known aggregation operators for learning privacy preferences on Android.

VI. The rest of the article is structured as follows: In Section 2, we review and discuss access control management approaches applied to Android. In Section 3, we give an overview of decision support system and we present the generic architecture²² of Kapuer. Section 4 introduces Kapuer's problem-solving model and its instantiation to the Android permission management context²³. In Section 5, we detail the learning algorithm Kagop. In Section 6, we introduce some features that complement the learning process of privacy preferences. We evaluate, in Section 7, Kapuer and Kagop on a real life scenario. Finally, we conclude in Section 8.

8. Conclusions

VII. We have presented in this article a custom permission management system for Android 4.4. Unlike other approaches, Kapuer does not only provide a way to modify what permissions an application can use. It learns from users' behavior to help them and advise them by proposing rules with different levels of abstractions. This way, they can protect their privacy more easily, without needing knowledge about access control models or policy's structure. We have also presented a detailed description of our learning engine. Kagop exploits all the concepts of our problem-solving model to take into account interactions and conflicts between criteria. Compared to two other methods, Kagop achieved good results. Evaluations on Kapuer show that hundreds of permissions can be handled with a limited number of actions by using abstractions.

VIII. The current version of Kapuer runs on Android 4.4. For the moment, each time a request is denied, Kapuer makes Android act as if the application does not have the permission. Since developers of Android 4.4 applications do not manage this case, some applications crashed. This issue will be resolved on Android 6.0 because now developers shall handle permission verification²⁴ before trying to use it. We will also take advantage of the new Android permission request interception²⁵ to implement our interactions with users. Finally, we

will integrate new Android 6.0 information (protection levels and groups of permission) as meta-criteria. As a consequence, Kapuer will be easier to maintain.

IX. One of the initial goals when we designed Kapuer was to inform people about privacy risks. For longer term research, we want to go further in that direction and not only inform people but also educate them about privacy issues. As an example, we need to explain them the consequences of granting some permissions to an application using approaches like privacy mirrors. The more people understand these risks, the better their privacy decisions will be.

X. Finally, Kapuer learns users preferences from scratch. A significant number of requests is needed before any proposition can be made to the user. It is possible to improve the beginning of the learning phase by initializing the system. Making surveys with different kind of users can help to find the best way to initialize these users' preferences.

NOTES

1. “The right to be let alone” (American lawyers Samuel D Warren and Louis D Brandeis 1890) – право на личную жизнь.

2. Dissemination of personal information – распространение личных данных.

3. To avoid intrusion/decisional interference – не допускать намеренного посягательства.

4. We performed an analysis – нами был проведен анализ.

5. Can directly harm privacy – могут нанести прямой вред частным интересам.

6. Under the guise of providing some services – под видом предоставления услуг.

7. To have access to the identity information – получить доступ к личным данным.

8. The privacy policy – политика конфиденциальности.

9. Collects personal and activity data – собирает и хранит личные данные и данные об активности в сетях.

10. Controlling access to applications – управление доступом к приложениям.

11. Granting all the permissions – предоставление всех разрешений.
12. Permission(s) management – управление разрешениями.
13. Either you authorize everything or you cancel the installation – либо вы разрешаете доступ ко всему, либо отменяете эту установку.
14. The basic native Android system – базовая система Андроид.
15. An Identity-Based Access Control model (IBAC) – модель контроля за доступом, основанная на фиксации идентичности.
16. A recommender-based system – система рекомендаций.
17. Assistant – помощник.
18. Aggregation operator – оператор агрегации (накопления).
19. To capture users` preferences in terms of privacy – улавливать предпочтения пользователей в отношении конфиденциальности.
20. The final Android implementation – последнее воплощение Андроид.
21. The cornerstone of our learning algorithm – краеугольный камень (основание) нашего обучающего алгоритма.
22. Generic architecture – обобщенная архитектура (сети).
23. Instantiation to the Android permission management context – соответствие контексту управления разрешениями в Андроид.
24. Permission verification – проверка необходимости разрешений.
25. The new Android permission request interception – новая функция Андроид по перехвату запросов доступа (на разрешение).

2. In the text find words and phrases with the following meanings, using the paragraph number.

Para X

great
 supposition
 to make something better
 starting
 likes and dislikes
 from the very beginning

Para VII

showed
 as distinct from
 give a way
 take into consideration
 estimations

Para IX

aim
investigation
teach
scientific problem
result
give permissions
methods

Para VIII

contemporary
handle
collapse
profit by
at last

Para IV

without reducing
ability to perform
difficult
helps
new
named

Para III

set up
abolish
to improve
a built-in system

Para II

a ruling place
carried out an analysis
leads to
Para I
promote
doubt

1. Describe the framework of the paper (Paras V, VI). Make up a list of mental action verbs.

2. Make up a complete list of connective elements across the text including the words mentioned in task 1 A.

How to write an abstract

1. Every author should know how to write a good abstract for both conference and journal papers.

2. It consists of: motivation, problem statement, approach, results, and conclusions.

Each section is typically a single sentence.

Motivation:

Why do we care about the problem and the results? This part should include the importance of your work, the difficulty of your area, and the effect it might have if successful.

Problem statement:

What problem are you trying to solve (a generalized approach, or for a specific situation)?

Approach:

How did you solve the problem (using simulation, analytic models, prototype construction, or analysis of field data)?

Results:

What's the answer? Avoid vague results such as "very", "small", or "significant", put the result in numbers.

Conclusions:

What are the implications of your answer? Are your results general, potentially generalizable, or specific to a particular case? Or just useless?

3. An abstract word limit should be 150-250 words.

4. You should have the phrases and keywords that people could use looking for your work.

5. Keywords should coincide with a particular category of a journal, or a conference topic area.

1. Read and translate the abstract of the article.

2. Write the analysis of the abstract to identify its parts in accordance with the recommendations given above. Remember to check up the word limit.

3. Try and complete the abstract with the sentences of your own.

HONEYPOTS AND HONEYNETS: ISSUES OF PRIVACY

ABSTRACT

Honeypots¹ and honeynets² are popular tools in the area of network forensics^{3a}. The deployment^{4a} and usage of these tools are influenced by a number of technical and legal issues, which need to be carefully considered. In this paper, we outline the privacy issues of honeypots and honeynets with respect to their technical aspects. The paper discusses the legal framework⁵ of privacy and legal grounds to data processing. We also discuss the IP address⁶, because by EU law, it is considered personal data. The analysis of legal issues is based on EU law and is supported by discussion on privacy and related issues.

Key words: Personal data, EU law, Honeypot, Privacy, IP address

4. Read the article, discuss the following questions in groups:

1. Are there Russian equivalents of the words *honeypots* and *honeynets*?
2. Could you give the definition of forensics ?
3. What sides of life does the legal framework of information traditionally include?
4. Why is the idea of personal data so urgent nowadays?
5. What risk for privacy do the honeypots and honeynets imply?
6. What types of the collected data can directly harm your privacy?
7. What does the principle of “purpose limitation” mean?
8. What is the advantage of the anonymization of data?

1. Introduction

I. The landscape of cybersecurity⁷ threats is continuously evolving⁸ and reactive security measures are often not sufficient for protecting information infrastructures. We continuously have to learn about new threats to keep pace with⁹ potential attackers¹⁰.

II. One of the most popular methods of learning about attackers is using *honeypots*. Spitzner defines honeypots as an information system resource whose value lies in an unauthorized or illicit¹¹ use of that resource. It can also be defined as a computing resource whose

value is in being attacked. A honeypot is deliberately¹² allowed to be compromised, and the attack is then analyzed so that we can learn about the methods, procedures, and tools that the attacker used.

III. It is unquestionable that honeypots increase our understanding of malicious^{13a} activity in cyberspace. However, we have to keep in mind that there are legal issues regarding honeypots that need to be addressed when deploying^{4b} one, analyzing the captured data, and sharing the results with others. One of the major legal issues is the issue of privacy, which we address in this paper. This issue influences how a honeypot can be deployed, what data they are allowed to collect, and what we can do with the collected data.

IV. To formalize the scope¹⁴ of our work, two research questions are stated:

1. What data are legally allowed to be collected by honeypots?
2. What are the legal conditions for the collection of data and data retention¹⁵?

V. In this paper, the authors focus on the European Union (EU) regulations¹⁶. The aim of this paper is to elaborate on¹⁷ the legal framework of the European Union. We acknowledge that cybersecurity is a global issue where information must be shared across borders and thus there are many legal implications¹⁸ which must be considered within different legal cultures. However, this question is out of the scope of the presented work and will be a subject of future research.

VI. This paper is organized into five sections. The background¹⁹ of honeypots and the related works are discussed in Section 2. This section focuses on previous literature related to the legal aspects of honeypots and honeynets, especially the issue of privacy. Section 3 is the main part of this paper and deals with privacy and personal data protection. Section 3.1 focuses on the legal framework of privacy and personal data protection in the EU law. Section 3.2 discusses the basic concepts of personal data protection in the EU. Section 3.3 is focused on the data collected by honeypots and honeynets from the perspective of the EU law. IP addresses as the most important collected data are discussed in Section 3.4. Section 3.5 deals with the legal grounds for data processing and purpose limitation²⁰.

In Section 4, the paper outlines issues related to privacy, namely network monitoring²¹ (Section 4.1) and the publication of results (Section 4.2). Section 5 concludes the paper and outlines the newly opened problem for future research.

2. State of the art²²

VII. In this section, we present the current state of the art in the discussed topics. First, we introduce honeypots to provide a background in the field. Second, the related work on honeypots and legal issues of honeypots will be presented.

2.1 Background on honeypots

VIII. For the purpose of this paper we classify honeypots according to their level of interaction and purpose. The first classification is based on level of interaction. The *level of interaction* can be defined as the range of possibilities that a honeypot allows an attacker to have. Low-interaction honeypots²³ detect attackers using software emulation^{24a} of the characteristics of a particular operating system and network services on the host operating system^{25a}. The advantage of this approach is better control of attacker activities, since the attacker is limited to software running on a host operating system. On the other hand, this approach has a disadvantage: a low-interaction honeypot emulates^{24b} a service, or a couple of services, but it does not emulate a full operating system.

IX. In order to get more information about attackers, their methods, and attacks, we use a complete operating system with all services. This type of honeypot is called a high-interaction honeypot^{26a}. This type of honeypot aims to give the attacker access to a real operating system, where nothing is emulated or restricted.

X. Spitzner suggests the classification of honeypots by *purpose*. There are research honeypots²⁷ and production honeypots²⁸. The research honeypot is designed to gain information about the blackhat community²⁹ and it does not add any direct value to the organization, which has to protect its information. The main aim here is to get maximum information about the blackhats by giving them full access to penetrate the security system³⁰ and infiltrate³¹ it.

A second type of purpose classified honeypot is the production honeypot, used within an organization's environment to protect the organization and help mitigate risk³². An example of the production honeypot is a honeypot which captures, collects, and analyzes malware for anti-virus systems, intrusion detection system signatures³³, etc.

XI. *HoneyNet* extends the concept of a single honeypot to a highly controlled network of honeypots. A honeyNet is composed of four core elements:

*Data control*³⁴ – monitors³⁵ and logs³⁶ all of the activities of an attacker within the honeyNet

*Data capture*³⁷ – controls and contains the activity of an attacker

*Data collection*³⁸ – stores all captured data in one central location

Data analysis – the ability of the honeyNet to analyze the data being collected from it

XII. The deployment and usage of honeypots bring many benefits³⁹, e.g. the possibility of discovering new forms of attacks. In addition, low-interaction honeypots are easy to deploy, undemanding resource-wise⁴⁰, and simple to use. On the other hand, a number of issues need to be addressed during the deployment and usage. The most frequent problems are:

XIII. *Inaccurate results* – in some cases, the data obtained from the honeypots lead to poor results, due to a limited amount of data

*Discovery and fingerprinting*⁴¹ – the attackers can detect the honeypots

*Risk of takeover*⁴² – the honeypot may be used to attack against the real (non-honeypot system)

XIV. The quantity and quality of the data collected from honeypots are one of the problems associated with their usage. This problem is closely linked to the *issue of privacy*. It represents one of the most significant concepts in the field of law, and it was set forth⁴³ in Article 8 of the European Convention on Human Rights. Privacy can be defined as the right to be left alone and to have a private life. It can also be defined as the right of a person to be free from unwarranted publicity⁴⁴.

XV. This includes some individual privacy, such as the privacy of the home and office, the protection of physical integrity⁴⁵, and also

the privacy of communications⁴⁶ (telephone calls, chats, emails etc.). Therefore, the primary motivation for writing this paper is the fact that an administrator has to take into account the issue of privacy and related issues in the process of data collection. The failure of an administrator to meet that responsibility leaves them open to a lawsuit⁴⁷ for any disruption of privacy⁴⁸ and resulting damages⁴⁹.

2.2 Related works

XVI. The papers dealing with the legal aspects of honeypots and honeynets focus on three fundamental legal issues of the deployment and usage of honeypots: privacy, liability⁵⁰, and entrapment⁵¹. We discuss them in more detail below. They only deal with privacy in the context of honeypots only. Most of papers focus on legal issues from the US law and from the perspective⁵² of the EU law.

XVII. The papers discussed deal directly with honeypots. There are a number of papers focusing on the legal aspects in related fields, such as digital forensics^{3b} and cybersecurity.

XVIII. Since honeypots belong to network forensics tools, the legal aspects of digital forensics are relevant⁵³. They include property law⁵⁴, constitutional law⁵⁵, tort law⁵⁶, contract law⁵⁷, cybercrime⁵⁸, criminal procedure⁵⁹, evidence law⁶⁰, and cyberwar⁶¹. An interesting paper is about legal and technical issues of Internet forensics^{3c}. It provides a combined approach on the major issues pertaining to⁶² the investigation of cybercrimes and the deployment of Internet forensics techniques. The paper also discusses the implications of data mining⁶³ techniques and the issue of privacy protection with regard to the use of forensics methods.

XIX. Another related field of research is *cybersecurity*. It focuses on such issues as infected hosts^{25b}, testbeds⁶⁴, non-isolated hosts^{25c}, publishing results, etc. There are also papers focusing on several US laws prohibiting or restricting network monitoring and the sharing of records⁶⁵ of network activity.

3. Privacy and personal data protection

XX. In this section we discuss some aspects of privacy and data protection in the area of honeypots. First, we outline framework

of privacy in the EU law. Then we discuss privacy issues concerning data collected by honeypots, IP addresses, and data processing.

3.1 Basic concepts of personal data protection

XXI. The data protection system is based on the principle of preventing privacy harm. To achieve this, the Data Protection Directive⁶⁶ incorporates a very broad definition of “personal data”, so the highest possible number of persons can be considered “data controllers”⁶⁷. The most important duty of the controller is to process personal data only for legitimate⁶⁸ and legal purposes and based on a legitimate legal ground. All this combined can ensure a high level of protection.

XXII. *Personal data* is defined as follows: “any information relating to an identified^{69a} or identifiable^{69b} natural person; an identifiable person is one who can be identified, directly or indirectly.” The most relevant part of the definition is the notion of indirect identifiability^{69c}. It means that any information, which can be used in the right context for the identification^{69d} of a person (“data subject”) is personal data, even though the information in itself (outside the right context) does not directly identify the data subject. This approach is necessary for assuring a high level of protection, but it leads to a situation where almost any information could be personal data. Thus, operators of honeypots and honeynets should be aware of this situation.

XXIII. A *purpose* is the cornerstone of every personal data processing. It is set by the data controller and all that happens to the data during its life cycle is connected with the set purpose. Personal data can be processed only in order to achieve the declared purpose, which has to be conveyed to the data subject. The personal data can also be retained only for a time period that is necessary for fulfilling that purpose. This principle is called “the purpose limitation”.

XXIV. The Data Protection Directive recognizes several legal grounds for data processing, from which the following is relevant for the case of honeypots and honeynets: the data subject has unambiguously given their consent⁷⁰.

XXV. The Data Protection Directive sets four conditions for the validity⁷¹ of consent which must be met. It has to be *freely given, specific, informed, and unambiguous*.

3.2. Collected data

XXVI. Almost any data collected by honeypots might be considered personal data. The first aspect of privacy issues within honeypots and honeynets is the type of data that is being collected. There are two general categories: a) the contents of communications; b) information to establish communication.

XXVII. The first type of collected data, the contents of communications (content data⁷²), is regulated by the Directive. Examples of content data are the bodies of email messages, file contents, full packets captured on a network segment, reconstructed content of interactive sessions⁷³ (e.g. command executed in a shell account⁷⁴, typed passwords), etc.

XXVIII. The extent⁷⁵ of the collected content data records is related to the honeypot's level of interaction. *Low-interaction honeypots* capture and collect smaller amounts of content data records than *medium-interaction*^{26b} and *high-interaction honeypots*.

XXIX. The second type of collected information records is *the information to establish communication* (no-content data, transactional data⁷⁶, also known as *metadata*⁷⁷). These are mostly traffic⁷⁸ and location data⁷⁹, which are defined as follows:

Traffic data – any data processed for the purpose of conveying a communication⁸⁰ on an electronic communications network⁸¹

Location data – data processed in an electronic communications network, indicating the geographic position of the terminal equipment⁸² of a user, of a publicly available electronic communications service⁸³

XXX. Examples of transactional data are IP addresses, network ports, network protocols, account names, email header information⁸⁴, time, date, website URLs⁸⁵, etc. The categories of transactional data retained in honeypots include:

Data necessary to trace and identify *the source and destination of a communication*, for example the IP address and domain name⁸⁶

Data necessary to identify *the date, time, and duration of a communication* (e.g. timestamp⁸⁷)

Data necessary to identify *the type of communication*, for example an Internet protocol (e.g. ftp⁸⁸, ssh⁸⁹, samba⁹⁰)

Data necessary to identify *the users' communication equipment* or what purports to be⁹¹ their equipment, for example the operating system

3.3 IP addresses

XXXI. In this section we argue that *IP addresses are personal data* in the meaning of the law. As stated before, the IP address is a piece of information necessary to trace and identify the source of a communication.

XXXII. An IP address is connected with a specific device. However, in many cases, we can assume a strong connection between the device and its user. That is the case of smartphones, tablets and other smart handheld devices, as well as personal computers. IP addresses are used by electronic communications service providers to help identify a subscriber. IP addresses are also collected and stored by electronic communications providers for the purpose of a possible criminal investigation⁹². IP addresses are used as information which leads to the identification of a person. Therefore, it counts as⁹³ indirectly identifying personal data.

XXXIII. Some courts have another opinion of the IP status. Their reasoning is as follows: IP addresses are not personal data in the situation of honeypot and honeynet operators, because the particular natural person is not identifiable by the means the operator has at their disposal. Furthermore, in most situations, the attack is carried out by a machine, not a human. In this case an identification of the natural person is fairly difficult.

XXXIV. However, in our opinion, it is safer to consider IP addresses personal regardless of what other information the operator has. There are two reasons for that. First, it is the basic preventive principle⁹⁴ of the personal data protection system, which regulates the amount of collected data, so it cannot be connected and misused. Second, even though in a number of cases the IP addresses can be connected only to a device and not a human being (e.g. the Internet of things⁹⁵), there is not an easy way for the honeypot operator to distinguish them.

3.4 Legal grounds to process data and purpose limitation

XXXV. IP addresses collected during the operation of honeypots and honeynets can be personal data of either the operator's customers or third persons, whose devices are used for the attack. The customers can provide consent for the personal data processing, but that is not the case for the third persons. Furthermore, it is advisable to rely on a different legal ground for processing than for consent, when it is available and applicable. The legal ground must be chosen according to the purpose of the processing.

XXXVI. The following may be considered *a relevant purpose* of personal data processing within honeypots and honeynets:

For *production honeypots* – safeguarding⁹⁶ the security of the service

For *research honeypots* – research and prevention of future threats

XXXVII. In the first case, the data controller can rely on their legitimate interest in the cyber security of his network. The possible harm of privacy for the data subject (those whose IP addresses are processed) is very little. Furthermore, this processing is also in accordance with the legitimate interest of the owners whose devices are used for the attack, since this processing might help to solve their unfortunate situation⁹⁷.

XXXVIII. In the second case, the situation is more complicated. The legitimate interest of the controller might be a promotion⁹⁸ of cyber security and a right to carry out their business properly. These interests must be proportionate with⁹⁹ the right of data subjects for privacy protection in the light of the possible harm done by the processing. Since the possible harm is quite low, we are convinced that the legal ground for processing established in the Directive should be applicable in the case of research honeypots as well.

4. Other privacy issues

4.1 Network monitoring

XXXIX. Another set of issues associated with the daily functioning honeypots and the realities of their operation is related to the very nature of honeypots in the area of research. A monitoring network may contribute to¹⁰⁰ its improved security or valuable

research output¹⁰¹, whether we are talking in terms of production or research honeypots. There are several questions to deal with, namely the proportionality of the invasion of data¹⁰² for research purposes or for security. Monitoring every single packet may lead to considering this kind of situation a threat in itself (the question on who will control the guards¹⁰³), although we point out that courts will look at industry practices¹⁰⁴.

XL. Although we were discussing issues related to clashes of values¹⁰⁵ and their legal quality in previous sections, we have not put focus on policy issues related to implied risks¹⁰⁶, which are related to the volume of data. If we take a look at this in the light of data retention, the retention of data for considerably long periods of time leads to risk exposure¹⁰⁷, which will pose a long-term threat to privacy and security to guarantee privacy rights in practice.

XLI. If data are stored, if all traffic is stored or monitored, then a leak of these data is a probable threat and a theft of these data is more probable the longer the period of time, because nothing is perfectly secure on the Internet and risks will become more salient¹⁰⁸ as the time for their emergence and chance to occur increases. By trying to be in a state of higher security, we are actually risking more by creating implied insecurity¹⁰⁹. Thus, efforts to maintain more secure societies may lead to societies which will have to face environments with higher risks and fewer factual¹¹⁰ securities, because their data will be exposed to these risks for longer periods of time. This means that protection cannot cross a certain line¹¹¹; it must be proportionate. These conclusions could be summarized as follows: if there is an absolute, large amount of information stored; the risk of it being stolen grows with time and volume. In other words, the internet is not perfect and security systems can be invaded, attacked, and penetrated successfully. This argument is quantitative in its essence.

XLII. A qualitative argument could be derived from different situations. What if a honeypot worked as a support facility¹¹² to a chat server or another electronic service and research and security would require specific data? This leads to another problem which arises in cases of secrecy of correspondence¹¹³. Even a network security and public order provisions¹¹⁴ should not deprive us of this right.

4.2 Publication of the results

XLIII. One of the important problems within this issue is the sharing and publishing of network traces. The scientific motivations for sharing these data are compelling¹¹⁵: common datasets¹¹⁶ can provide meaningful¹¹⁷ comparisons between competing research approaches; simulated data¹¹⁸ are inadequate for some uses; and existing datasets may not reflect present day threats or traffic characteristics. In this aspect, it is necessary to mention the anonymization issue. Before presenting research data, it is necessary to anonymize these data. Network trace¹¹⁹ anonymization¹²⁰ is an active area of research in the security community, as shown by the ongoing¹²¹ development of anonymization methods and the releases¹²² of network data that they enable. Since the results contain personal data, their publication would constitute a new personal data processing with a new purpose and legal ground. Since this might be quite problematic, it is recommended to publish only anonymized version of the results.

XLIV. The publication of results also has the potential to harm an organization's reputation by revealing network details that the institution would prefer to keep secret. A strictly legal concern¹²³ that this raises is the potential for a breach of contract¹²⁴. The possibility that a publication will reveal details about a honeypot or a production network also raises liability issues. Honeynet administrators should also consider whether the papers or datasets that they publish could reveal information that could help adversaries¹²⁵ attack the honeynet or production network of an organization. Publishing datasets is likely to pose a greater risk to a production network than a paper; therefore, data releases may deserve a more careful vetting¹²⁶ by IT officers than papers do. Another aspect of liability is the fact that the publication of results merely provides information that might help another person commit cybercrime.

5. Conclusions

XLV. The legal aspects of honeypots and honeynets are a fascinating research topic. In this paper, we have discussed the aspects of privacy and personal data protection. The paper has outlined the concept of personal data protection in the EU law and focused on the issues

of the purpose of data processing, the legal grounds for data processing, and the retention of data. The paper has also discussed issues related to privacy, such as network monitoring and the publication of results.

XLVI. The conclusions of this paper open issues that need to be addressed in the context of future research. In connection with the fact IP addresses are personal data, it is necessary to discuss them in more detail and propose an anonymization technique for the collected data. Other newly opened research questions are closely linked to international cooperation and the cooperation with private and public authorities. In these cases, it is needed to closely discuss the issue of cross-border transmission of data¹²⁷.

NOTES

1. Honeypot – ресурс-приманка (ловушка) для злоумышленников, цель которой состоит в том, чтобы быть исследованным, атакованным, использованным.

2. Honeynet – сеть машин с системами, используемыми в повседневной деятельности, но предназначенными для компрометации, в процессе которой информация фиксируется, а затем анализируется. Может быть использовано множество систем одновременно.

3. a) Network forensics – система мониторинга и анализа сетевого трафика (сетевая криминалистика, экспертиза).

b) Digital forensics – цифровая (компьютерная) криминалистика (расследование инцидентов).

c) Internet forensics – криминалистическая компьютерная экспертиза следов пребывания в Интернете.

4. a) Deployment – применение, использование;

b) Deploy – применять, использовать.

5. Legal framework – законодательная база.

6. IP address – Internet protocol address – адрес интернет-протокола.

7. Cybersecurity – информационная безопасность.

8. Evolve – эволюционировать.

9. To keep pace with – не отставать от, держаться наравне.

10. Attacker – взломщик.

11. Illicit – противоправный, незаконный, запрещенный.
12. Deliberately – намеренно.
13. a) Malicious – злоумышленный;
b) malware – программное обеспечение для взлома (хакерская программа, вредоносный код), вредоносное ПО.
14. To formalize the score – упорядочить (объем и содержание); оформить рамки.
15. Data retention – запоминание (сохранение и хранение) данных.
16. Regulations – нормативно-правовые акты, положения.
17. To elaborate on – подробно рассказывать, раскрыть тему о.
18. Implications – осложнения, последствия
19. Background – история вопроса (проблемы).
20. Purpose limitation – ограничение прав (в распространении личных данных).
21. Network monitoring – сетевой мониторинг (текущий контроль сети).
22. State of the art – современное состояние.
23. Low-interaction honeypots – приманки слабого взаимодействия (направлены на обнаружение несанкционированных попыток соединения и сбор данных об известных атаках).
24. a) Emulation – эмуляция (имитация);
b) to emulate – имитировать.
25. a) Host operating system – операционная система хоста (сервера виртуальных машин).
b) Host – хост, ведущий вычислительный узел; устройство, предоставляющее сервисы формата «клиент–сервер» (компьютер, сервер, подключенный к глобальной или локальной сети).
c) Non-isolated host – взаимосвязанный хост.
26. a) High-interaction honeypots – высокоинтерактивные приманки (сильного взаимодействия) (предоставляют злоумышленнику доступ к реальной операционной системе, где нет имитации или ограничений).
b) Medium-interaction honeypots – приманки среднего взаимодействия (предоставляют злоумышленнику доступ к виртуальной операционной системе, которая контролируется

реальной операционной системой; осуществляет сбор программных средств злоумышленника).

27. Research honeypot – исследовательская ловушка, направленная на сбор данных о злоумышленнике.

28. Production honeypot – производственная ловушка, помогающая снизить риск, оказывающая влияние на обеспечение безопасности систем и сетей. Полученные данные могут быть использованы для предупреждения, обнаружения, протоколирования.

29. The blackhat community – сообщество «черных шляп» (вид хакеров, киберпреступники).

30. To penetrate the security system – проникать внутрь системы безопасности.

31. To infiltrate – внедриться.

32. To mitigate risk – минимизировать риск, снизить (свести у минимуму).

33. Intrusion detection system signatures – записи системы обнаружения несанкционированного проникновения, системы обнаружения хакерских атак.

34. Data control – управление данными (удержание под контролем их пересылки).

35. To monitor – фиксировать, следить за состоянием.

36. To log – протоколировать, регистрировать.

37. Data capture – сбор данных (фиксация всех действий злоумышленника).

38. Data collection – накопление данных.

39. Benefits – положительные стороны, плюсы.

40. Undemanding resource-wise – не требующий разумного (умелого, грамотного) использования ресурсов.

41. Fingerprinting – зд. оставление следов, отпечаток пользования.

42. Takeover – захват, взятие под контроль злоумышленником.

43. To set forth – объясняться.

44. Unwarranted publicity – необоснованное внимание общества (публичность).

45. Physical integrity – телесная (физическая) неприкосновенность.

46. Communications – 1) средства общения; 2) информационный обмен (информационные материалы).
47. Lawsuit – судебные тяжбы (дела).
48. Disruption of privacy – нарушение конфиденциальности (приватности).
49. Damages – коммерческие санкции, возмещение убытков.
50. Liability – ответственность (обязательство).
51. Entrapment – провоцирование на уголовно наказуемое деяние.
52. From the (a) perspective – с точки зрения.
53. Relevant – важный, уместный, значимый, актуальный.
54. Property law – имущественное право.
55. Constitutional law – конституционное право.
56. Tort law – гражданское право.
57. Contract law – договорное (контрактное) право.
58. Cybercrime – кибер (компьютерное) преступление.
59. Criminal procedure – уголовно-процессуальное право.
60. Evidence law – доказательственное право.
61. Cyberwar – информационная война.
62. Pertaining to – имеющий отношение к.
63. Data mining – добывание данных, извлечение информации из данных, анализ данных, сбор сведений из массивов данных.
64. Testbed – испытательный образец, тестовая модель
65. To share the records (data) – делиться записями (информацией); совместно использовать информацию, обмениваться данными.
66. Data Protection Directive – директива (указание) о защите данных.
67. «Data controllers» – контроллеры данных.
68. Legitimate – законный (легальный, полноправный, подлинный).
69. a) Identified – опознанный, идентифицированный;
b) Identifiable – легко опознаваемый, идентифицируемый.
c) Identifiability – идентифицируемость, опознаваемость.
d) Identification – идентификация, установление личности.
70. Unambiguously give their consent – однозначно (ясно) давать согласие.

71. Validity – обоснованность, законность, юридическая сила.
72. Content data – данные о содержании.
73. Interactive session – диалоговый сеанс.
74. Shell account – учетная запись с доступом через оболочку.
75. Extent – объем, степень, размер.
76. Transactional data – данные об операциях.
77. Metadata – метаданные (данные о данных, напр.: структура файла; данные, относящиеся к дополнительной информации).
78. Traffic data – информация о трафике (потоке данных).
79. Location data – данные о расположении (местонахождении).
80. Conveying a communication – передача информации, распространение информации.
81. Electronic communication network – сеть электронных коммуникаций.
82. Terminal equipment – комплект коммуникационного оборудования для приема и передачи сигналов по линии или каналу связи.
83. Electronic communication service – служба электронной коммуникации.
84. Email header information – информация, содержащаяся в заголовке сообщения.
85. URL (Uniform Resource Locator) – электронный адрес размещения, сетевой адрес (ресурса сети).
86. Domain name – имя домена (доменное имя), название сайта, определенная буквенная последовательность, обозначающая имя сайта.
87. Time stamp – время создания (модификации) файла.
88. FTP protocol – File transfer protocol – стандартный протокол передачи данных.
89. SSH protocol – Secure Shell Protocol («безопасная оболочка») – сетевой протокол прикладного уровня, позволяющий производить удаленное управление операционной системой.
90. Samba – сетевой протокол прикладного уровня для удаленного доступа к файлам, к сетевым дискам и принтерам.
91. To purport to be – иметь видимость, по виду являться, быть заявленным как.

92. Criminal investigation – расследование преступных действий, возбуждение уголовного дела.

93. To count as – считаться, засчитываться за.

94. Preventive principle – предупредительная мера.

95. The Internet of things – интернет вещей, концепция вычислительной сети физических предметов, оснащенных встроенными технологиями для взаимодействия друг с другом или с внешней средой для исключения необходимости участия человека.

96. Safeguarding – обеспечение сохранности.

97. Unfortunate situation – проблемная ситуация.

98. Promotion – стимулирование, содействие.

99. To be proportionate with – быть соразмерным с.

100. To contribute to – способствовать.

101. Research output – результаты исследования.

102. Invasion of data – захват данных (посягательство на данные).

103. “Who will control the guards?”= “Who will guard the guards?” – (лат.) «Кто устережет самих сторожей?».

104. Industry practices – особенности отрасли, области.

105. Clashes of values – конфликт ценностей.

106. Implied risks – все вытекающие отсюда последствия, предполагаемые риски.

107. Risk exposure – подвержение риску, подверженность риску.

108. Salient – выраженный, существенный.

109. Implied insecurity – косвенная (потенциальная) скрытая небезопасность (слабая защита информации), уязвимость.

110. Factual – реальный.

111. Cross the line – выйти за рамки дозволенного.

112. Support facility – вспомогательный объект (оборудование), объекты технического обеспечения.

113. Secrecy of correspondence – тайна переписки.

114. Public order provisions – положения общественного порядка.

115. Compelling – основательный, востребованный, убедительный.

116. Dataset – пакет данных, набор данных.
117. Meaningful – ценный, полезный.
118. Simulated data – имитированные данные.
119. Network traces – трассировка сети (отслеживание сетевой активности, маршрутов следования данных в сетях).
120. Anonymization (of personal data) – обезличивание (персональных данных), процесс, при котором персональные данные меняются таким образом, что субъект не может быть прямо или косвенно идентифицирован оператором персональных данных.
121. Ongoing – непрерывный (постоянный).
122. Releases – публикация, разглашение информации.
123. Legal concern – юридические последствия.
124. Breach of contract – нарушение соглашения, невыполнение условий договора (контракта).
125. Adversary – злоумышленник.
126. Vetting – экспертиза (проверка).
127. Cross-border transmission – международная (трансграничная) зарубежная передача.

4. Read the article, discuss the following questions in groups:

1. Are there Russian equivalents of the words *honeypots* and *honeynets*?
2. Could you give the definition of forensics ?
3. What sides of life does the legal framework of information traditionally include?
4. Why is the idea of personal data so urgent nowadays?
5. What risk for privacy do the honeypots and honeynets imply?
6. What types of the collected data can directly harm your privacy?
7. What does the principle of “purpose limitation” mean?
8. What is the advantage of the anonymization of data?

5. Study Para VI and discuss the structure of the article with your partner. What similar sections does it have in comparison with the previous article? What descriptive verbs and phrases do the authors use to describe the contents of different sections?

6a. Study Para VIII and point out the most important parts in it:

a) the topic sentence (introduces the topic of the paragraph and states an idea or an attitude about the topic);

b) the controlling idea (the idea or attitude which controls what the sentences in the paragraph will discuss; it should be clear and focused on a particular aspect).

Eg. *Smoking cigarettes can be an expensive habit.* – a topic sentence.

Smoking can be expensive. – a controlling idea.

c) the support (the material used to support the opinion or attitude expressed in the topic sentence – factual detail (facts from resource material, such as magazines, journals, books; or the things we have observed).

d) transitions (*for example, however, also, to begin with, in contrast*).

6b. 1. Is this paragraph unified; that is, do all of the sentences support the controlling idea?

2. Is the paragraph coherent; that is, are the sentences logically arranged and do they flow smoothly (how well one idea or sentence leads into another)?

7. In the text find words and phrases with the following meanings, using the paragraph number.

Para I

constantly

enough

discover

Para III

indisputable

Para IV

issues

Para V

admit

use in common with others

still

Para XVIII

instruments

gives

Para XIX

limiting

Para XX

plan structure

Para XXI

injury

includes

permissible by law

guarantee

Para VI	consists of connected concerns in the context of summarizes	Para XXII	causes nearly
Para VII	to give the history of the problem	Para XXIII	is stated
Para VIII	the series of yet inconvenience complete	Para XXIV	certainly, without question
Para IX	is used to	Para XXV	particular
Para X	offers to obtain	Para XXVII	written communication
Para XI	basic place	Para XXIX	mainly
Para XII	also several common	Para XXX	held on
Para XIV	related to (2) «The right to be let alone»	Para XXXII	intense link
Para XV	so inability to cope with one's duty	Para XXXIII	rather
		Para XXXIV	applied wrongly
		Para LI	opening of information stealing of
		Para LII	take away something
		Para LIV	has the possibility just
		Para LV	interesting

Part III

tOPICS FOR speaking AND DISCUSSION

MY SCIENTIFIC WORK

1. Hello! Let me tell you some words about myself and my scientific work.

2. My name is ...

3. Last year I got the Bachelor's Degree in (Radiophysics, Information and communication technologies and systems, Radioengineering, Physics, Electronics and Nanoelectronics).

4. The same year I decided to enter the Master's program (Information security; Cybersecurity).

5. This field (of physics) studies...

6. As a student I was interested in theoretical and practical aspects ...

7. That is the reason why I chose to continue research work in the field of ...

8. I suppose the question of ... is up-to-date and quite urgent nowadays because it is considered to be the basis of (it can help to solve ecological and social problems) ...

9. Therefore, the subject-matter of my future thesis is ...

10. I perform my investigation under my scientific supervisor.

11. He is Doctor of ... (Candidate of ...), Professor of ... (Associate Professor of ...) the Department of ...

12. The aim of my study is to (analyze, work out, consider)...

13. In order to reach this aim, I am going to set the following tasks:

a) Firstly, the ... should be evaluated.

b) Secondly, ... are to be outlined.

c) Thirdly, it is important to investigate

14. In order to carry out the work I am going to read and analyze home and foreign literature, connected with the topic of my future dissertation.

15. I also plan to ...

16. I am going to write and publish papers on this topic, to participate in scientific conferences on... and to make reports.

MY EXPERIMENT

1. The experiment under study was devoted to the problem of ...
2. The main aim of our experiment was to show (find out, calculate, investigate, describe the properties).
3. In the process described, the methods of ... were used to observe ... and reveal ...
4. The experiment carried out (conducted, run), the following equipment (devices) was (were) to be employed:
5. ... (how many) stages could be traced in our research work.
6. Firstly, the hypothesis was formed. If ..., then
7. The hypothesis was tested under the certain conditions. For example (instance); (In particular),
8. Secondly, a primary run of the experiment was conducted.
9. ... was placed (put), was measured, were attached, was controlled, was separated from, were embedded (быть внедренным)/the measurements (calculations) were made.
10. The data collection of ...took place, followed by the data analysis of .../The data (the results of...) were presented (given, analyzed, compared with, collected).
11. In ... (how many) (days, weeks, months) the second run of the experiment was held.
12. The data of ... were interpreted and the following conclusions were drawn: .../The results agreed well with the theory.
13. The changes observed during ... supported the hypothesis.
14. It is urgent to mention that some problems occurred during the experiment: ...
15. They might be caused by
16. The results were presented in the form of graphs, figures, images, tables.
17. The table № ... showed

METHODS AND TECHNIQUES OF RENDERING

INTRODUCTION

1. The article I am going to give a review of is taken from...
2. The headline of the article is...
3. The author of the article is ...

STRUCTURE

4. The article is devoted to the problem of ... /The key issue of the article is .../As the title implies the article describes.../The paper is concerned with...

The message of the paper is that .../The main idea of the article is that...

5. The paper under discussion may be divided into several logically connected parts:

6. The first part contains the following facts.../looks at recent research dealing with...

7. The second part describes in details .../It is spoken in detail about...

8. I would like to mention briefly .../The text gives valuable information on...

CONTENTS

9. The author starts by telling the reader...

10. At the beginning of the article the author depicts.../It is reported that...

11. Touches upon...

explains

introduces

mentions

makes a few critical remarks

outlines

Much attention is given to/Some factors are taken into consideration/A brief account is given of/Reference is made to/It gives a detailed analysis of...

12. At the end of the paper the scientist dwells on...
points out
generalizes
reveals
exposes
gives a full coverage of

CONCLUSION

13. The researcher concludes by saying that ...
makes it clear
gives a warning that ...
draws a conclusion that ...
comes to the conclusion that ...
The following conclusions are drawn...

MY OPINION

14. Taking into consideration the fact that ...
15. In addition.../Furthermore...
16. On the one hand ..., but on the other hand ...
17. To come back to what I was saying ...
18. From my point of view/My own attitude to this article is...
19. I fully agree with/I don't agree with...
20. I have found the paper dull/important/interesting/of great value, because...
21. The article is of great help to/is of interest to...

Оглавление

PART I.....	3
DESCRIPTIONS OF HOW THINGS WORK: PURPOSE.....	3
CAUSE AND EFFECT.....	4
ACTIONS IN SEQUENCE.....	5
DEFINITIONS.....	8
PART II.....	10
APPLICATION OF READING STRATEGIES	10
SYSTEMS.....	10
THE SCOPE OF ECOLOGY.....	15
PART II.....	21
APPLICATION OF READING STRATEGIES TO INFORMATION SECURITY TEXTS.....	21
HOW TO WRITE AN ABSTRACT.....	28
HONEYPOTS AND HONEYNETS: ISSUES OF PRIVACY.....	29
PART III	49
TOPICS FOR SPEAKING AND DISCUSSION.....	49

Учебное издание

Составители:

Шульдешова Татьяна Васильевна

Пермякова Дарья Игоревна

**УЧИМСЯ ГОВОРИТЬ,
ПИСАТЬ И ДУМАТЬ
ПО-АНГЛИЙСКИ**

Практикум для магистрантов

Верстка Е. Б. Половкова

Технический редактор Л. Н. Селиванова

Подписано в печать 28.06.18. Формат 60×84 ¹/₁₆.

Усл. печ. л. 3,25. Уч.-изд. л. 1,9.

Тираж 3 экз. Заказ

Оригинал-макет подготовлен

в редакционно-издательском отделе ЯрГУ.

Ярославский государственный университет

им. П. Г. Демидова.

150003, Ярославль, ул. Советская, 14.

