ТЕСТИРОВАНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

ЮРИДИЧЕСКИ-ПРАВОВОЙ АНАЛИЗ

Олег Дубина, адвокат, партнер ЮФ «Современные правовые решения»

ITU Regional Workshop for Europe and CIS on Cybersecurity and Child Online Protection (Odessa, Ukraine, 4 to 6 April 2018)

СОВРЕМЕННЫЕ ПРАВОВЫЕ РЕШЕНИЯ

supri.pro

О чем речь ?

- Тесты на проникновение (pentest) понятие, виды и практика применения
- Тесты на безопасность - мировая практика правового регулирования
- Тестирование безопасности в украинском законодательно-правовом поле

ИССЛЕДОВАНИЕ БЕЗОПАСНОСТИ

ИССЛЕДОВАНИЯ БЕЗОПАСНОСТИ

PENETRATION TEST

метод оценки безопасности компьютерных систем или сетей средствами моделирования атаки злоумышленника

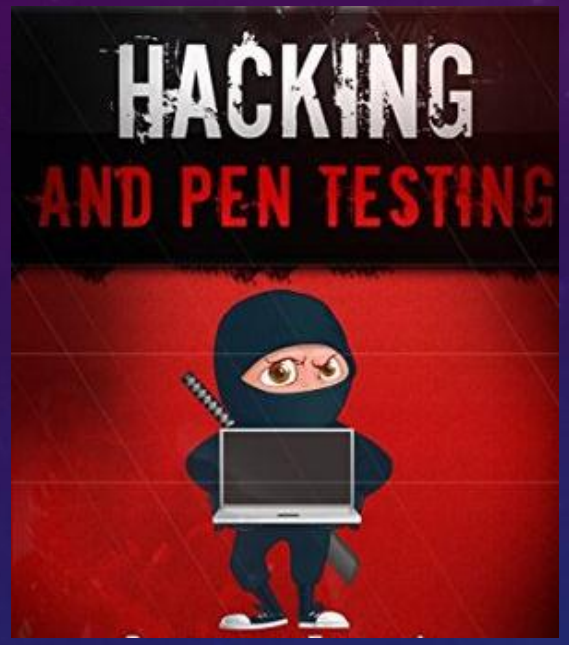
AUDIT

методика оценки на соответствие требованиям, лучшим практикам или рекомендациям нормативных актов, стандартов и документации производителей оборудования и ПО

AUDIT

Оценка соответствия информационной системы, её компонентов и процессов с какими-либо промышленными стандартами и «лучшими мировыми практиками», такими как, Cobit, стандартами серии ISO/IEC 2700x, рекомендациями CIS/SANS/NIST/etc и стандартом PCI DSS

PENETRATION TEST



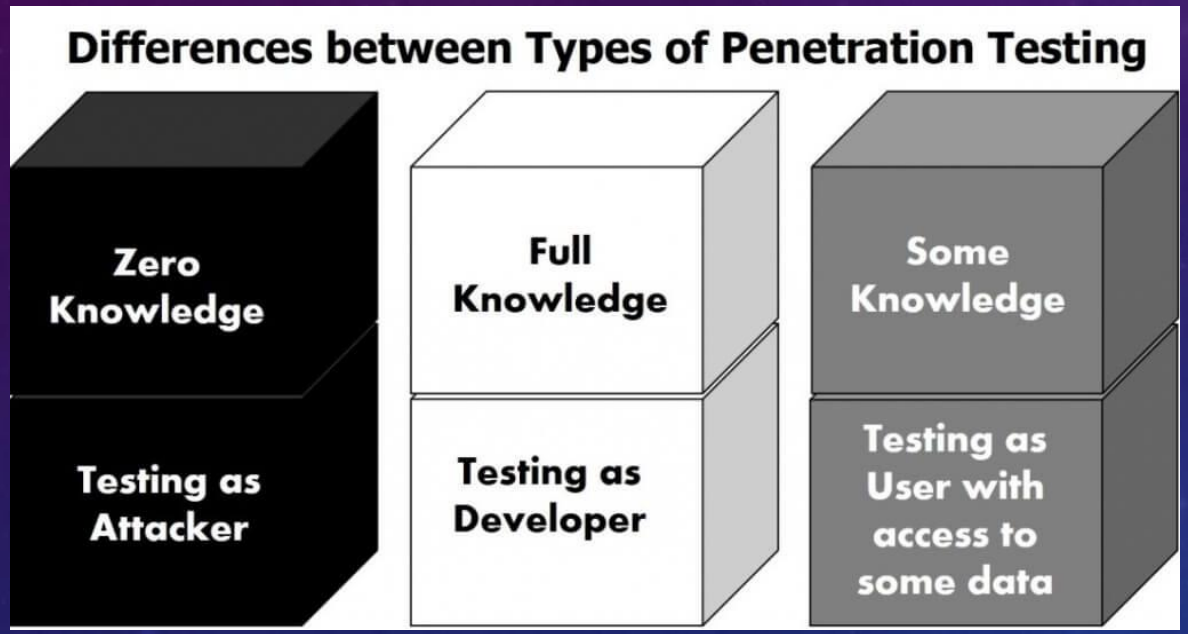
Набор методов и средств основанный на моделировании атаки злоумышленника. Включает в себя активный анализ системы на наличие потенциальных уязвимостей и их использование, анализ ведется с позиции потенциального атакующего и включает в себя активное использование уязвимостей системы.
Объектами тестирования могут быть как отдельные информационные системы, например: CMS (система управления содержимым), CRM (система управления взаимоотношениями с клиентами), интернет клиент-банк, так и вся инфраструктура в целом: периметр сети, беспроводные сети, внутренняя или корпоративная сеть, а так же внешний периметр.

PENETRATION TEST

Задача тестирования на проникновение — поиск всех возможных известных уязвимостей программного обеспечения (ПО), недостатков парольной политики, недостатков и тонкостей настроек конфигурации ИС. Во время подобного теста специалист устраивает псевдоатаку на сеть или инфраструктуру, инсценируя действия реальных злоумышленников или атаку, проводимую вредоносным программным обеспечением без непосредственного участия атакующего.

Целью данных тестов является выявление слабых мест в защите от подобных атак и устранение найденных в ходе псевдоатак уязвимостей.

ОСНОВНЫЕ ТИПЫ PENTEST`a



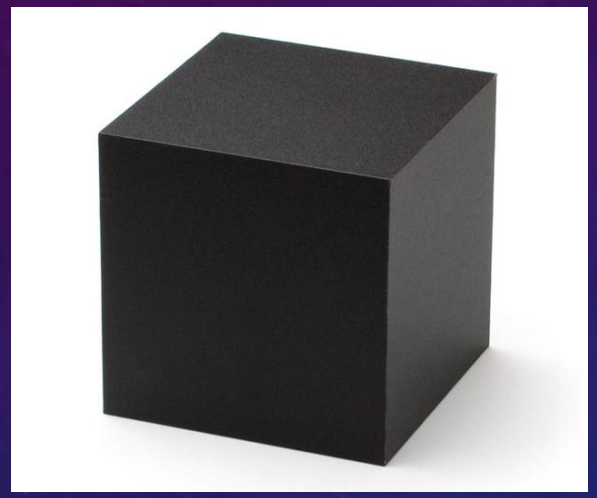
В зависимости от имеющейся изначальной информации об объекте исследования у тестировщика и методов его «атак» пентест принято разделять на категории

BLACK BOX

GREY BOX

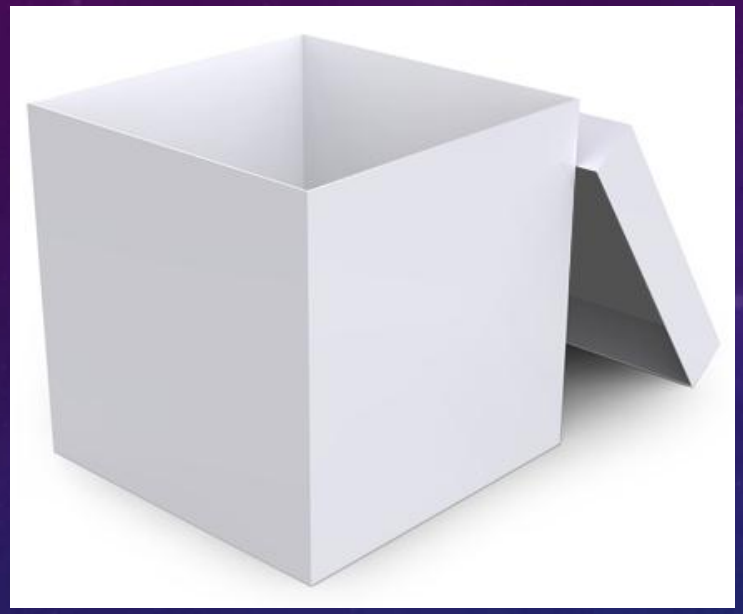
WHITE BOX

BLACK BOX PENTEST



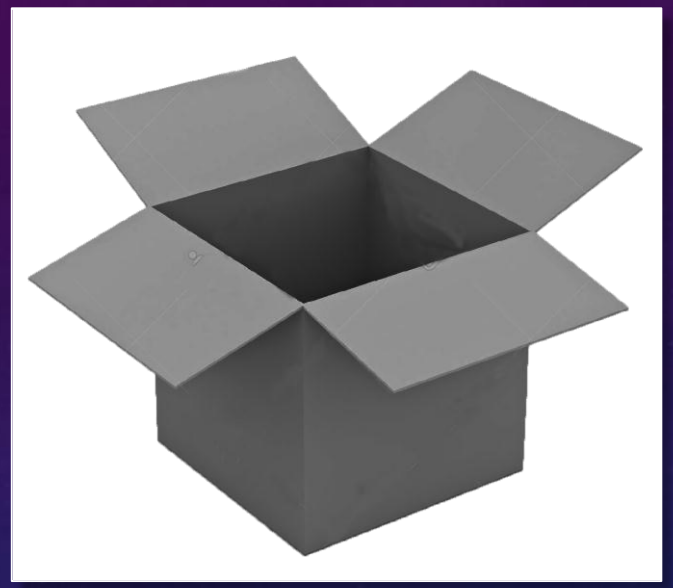
BlackBox — «черный ящик». Специалист располагает только общедоступной информацией о цели исследования, её сети и параметрах. Данный вариант максимально приближен к реальной ситуации. В качестве исходных данных для тестирования исполнителю сообщается только имя компании или ее сайт, а всю остальную информацию, такую как используемые компанией IP-адреса, сайты, точки выхода офисов и филиалов компании в сеть Интернет, исполнителю придётся выяснять самому

WHITE BOX PENTEST



WhiteBox – полная противоположность BlackBox. В данном случае, специалисту предоставляется максимум необходимой для него информации, вплоть до административного доступа на любые сервера. Данный способ позволяет получить наиболее полное исследование уязвимости объекта. При WhiteBox исполнителю не придётся тратить время на сбор информации, составления карты сети, и другие действия перед началом тестирования, а так же сократит время самого тестирования, т.к. часть проверок просто не придется делать. Плюс данного метода в более полном и комплексном подходе к исследованию. Минус в том, что это менее приближено к ситуации реальной атаки злоумышленника.

GREY BOX PENTEST



GrayBox – это средний вариант между WhiteBox и BlackBox, когда исполнитель действует по варианту BlackBox и периодически запрашивает информацию о тестируемой системе, для того чтобы сократить время исследования или более эффективно приложить свои усилия. Такой вариант самый популярный, так как позволяет провести тестирование без траты лишнего времени на сбор информации, и больше времени уделить поиску уязвимостей, при этом данный вариант остается достаточно близким к реальной ситуации действия злоумышленника.

ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ МИРОВАЯ ПРАКТИКА ПРАВОВОГО РЕГУЛИРОВАНИЯ

ЗАКОНОДАТЕЛЬСТВО США

Основной закон США, касающийся компьютерных преступлений, был сформулирован в 1986 г. и имеет наименование «О мошенничестве и злоупотреблениях, связанных с компьютерами».

Впоследствии состав «мошенничества с использованием компьютеров» вошел в Свод законов США

ЗАКОНОДАТЕЛЬСТВО США

LAWS ADDRESSING HACKING, UNAUTHORIZED ACCESS, COMPUTER TRESPASS, VIRUSES, MALWARE	
STATE	**CITE**
Alabama	Ala. Code §§ 13A-8-112, 13A-8-113
Alaska	Alaska Stat. § 11.46.740
Arizona	Ariz. Rev. Stat. §§ 13-2316,13-2316.01,13-2316.02
Arkansas	Ark. Code §§ 5-41-101 to -206
California	Cal. Penal Code § 502
Colorado	Colo. Rev. Stat. § 18-5.5-101 to -102
Connecticut	Conn. Gen. Stat. § 53a-250 to 53a-261
Delaware	Del. Code tit. 11,§ 931 to 941
Florida	Fla. Stat. § 815.01 to 815.07, §§668.801to .805
Georgia	Ga. Code §§ 16-9-90 to 16-9-94,§§ 16-9-150 to 16-9-157
Hawaii	Hawaii Rev. Stat. §§ 708-890 to 708-895.7
Idaho	Idaho Code §18-2201, § 18-2202
Illinois	720 ILCS § 5/17-50 to -55
Indiana	Ind. Code §§ 35-43-1-4, 35-43-2-3
Iowa	Iowa Code § 716.6B
Kansas	Kan. Stat. Ann. § 21-5839
Kentucky	Ky. Rev. Stat.§§434.840, 434.845, 434.850, 434.851, 434.853, 434.855, 434.860
Louisiana	La. Rev. Stat.Ann.§§ 14:73.1 to 14:73.8
Maine	Me. Rev. Stat. Ann. tit. 17-A, § 431 to 435
Maryland	Md. Code, Crim. Law § 7-302
Massachusetts	Mass. Gen. Laws Ann.ch. 266, § 33A
Michigan	Mich. Comp. Laws §§ 752.791, 752.792, 752.793, 752.794, 752.795, 752.796, 752.797
Minnesota	Minn. Stat. §§ 609.87 to 609.893
Mississippi	Miss. Code § 97-45-1 to 97-45-33
Missouri	Mo. Rev. Stat.§ 537.525,§ 569.095,§ 569.097,§ 569.099
Montana	Mont. Code Ann.§ 45-2-101,§ 45-6-310,§ 45-6-311
Nebraska	Neb. Rev. Stat.§§ 28-1341 to28-1348
Nevada	Nev. Rev. Stat. § 205.473 to 205.513
New Hampshire	N.H. Rev. Stat. Ann. §§638:16, 638:17, 638:18,638:19
New Jersey	N.J. Rev. Stat.§§ 2A:38A-1 to -3, § 2C:20-2, §§ 2C:20-23 to 34
New Mexico	N.M. Stat. § 30-45-1 to 30-45-7
New York	N.Y. Penal Law § 156.00 to 156.50

LAWS ADDRESSING DENIAL OF SERVICE ATTACKS	
STATE	**CITE**
Alabama	Ala. Code § 13A-8-112(5)
Arizona	Ariz. Rev. Stat. § 13-2316(4)
Arkansas	Ark. Code § 5-41-203(a)
California	Cal. Penal Code § 502
Connecticut	Conn. Gen. Stat. § 53a-251
Delaware	Del. Code tit. 11, § 934
Florida	Fla. Stat. § 815.06
Georgia	Ga. Code § 16-9-93
Illinois	720 ILCS § 5/17-51
Indiana	Ind. Code § 35-43-1-8
Louisiana	La. Rev. Stat. Ann. § 14:73-4
Mississippi	Miss. Code § 97-45-5
Missouri	Mo. Rev. Stat. § 569.099
Nevada	Nev. Rev. Stat. § 205.477
New Hampshire	N.H. Rev. Stat. Ann. § 638:17
North Carolina	N.C. Gen. Stat. § 14-456, 14-456.1
Ohio	Ohio Rev. Code § 2909.01
Oklahoma	Okla. Stat. tit. 21, § 1953
Pennsylvania	18 Pa. C.S.A. § 7612
South Carolina	S.C. Code § 16-16-10
Tennessee	Tenn. Code § 39-14-601
Virginia	Va. Code § 18.2-152.4
Washington	Wash. Rev. Code § 9A.90.060
West Virginia	W. Va. Code § 61-3C-8
Wyoming	Wyo. Stat. § 6-3-504

Кроме федерального законодательства США, касающегося компьютерных преступлений и безопасности, действует множество законов штатов, которые различны в каждом из штатов

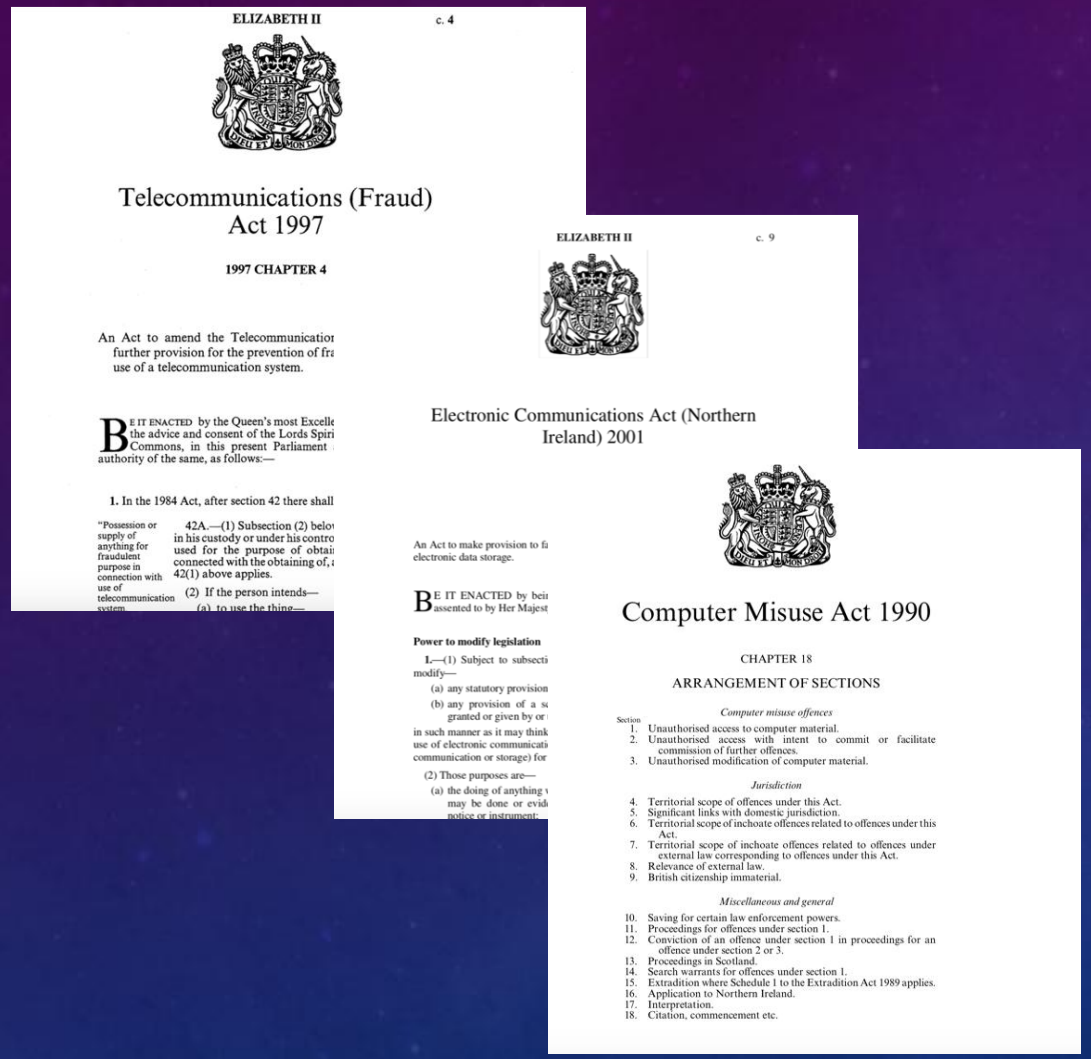
ЗАКОНОДАТЕЛЬСТВО США

Дело Scott Moulton президента компании «Network Installation Computer Services, Inc.», которого обвиняли в нарушении целого перечня законодательных актов:

- Georgia Unfair Trade Practices Act, O.C.G.A
- Section 10-1-372, Section 43(a) of the Lanham Act,
- 15 U.S.C. Section 1125(a), the Georgia Computer Systems Protection Act,
- O.C.G.A. Section 16-6-90 et seq.,
- Computer Fraud and Abuse Act, 18 U.S.C. Section 1030.

Суть обвинения это проведение сканирования портов подрядчика которое задело сервера сторонней фирмы.
Итог многолетние судебные разбирательства по итогам которых местные суды штата Джорджия признали Scott Moulton виновным, но Верховный суд в последующем полностью оправдал его.

ЗАКОНОДАТЕЛЬСТВО ВЕЛИКОБРИТАНИИ



ELIZABETH II c. 4

Telecommunications (Fraud) Act 1997

1997 CHAPTER 4

An Act to amend the Telecommunicatior further provision for the prevention of fra use of a telecommunication system.

BE IT ENACTED by the Queen's most Excelle the advice and consent of the Lords Spiri Commons, in this present Parliament authority of the same, as follows:—

1. In the 1984 Act, after section 42 there shall

"Possession or supply of anything for fraudulent purpose in connection with use of telecommunication system.

42A.—(1) Subsection (2) belo in his custody or under his contro used for the purpose of obtai connected with the obtaining of, 42(1) above applies.

(2) If the person intends—

(a) to use the thing—

ELIZABETH II c. 9

Electronic Communications Act (Northern Ireland) 2001

An Act to make provision to fa electronic data storage.

BE IT ENACTED by beir assented to by Her Majest

Power to modify legislation

1.—(1) Subject to subsecti modify—

(a) any statutory provision

(b) any provision of a s granted or given by or in such manner as it may think use of electronic communicati communication or storage) for

(2) Those purposes are—

(a) the doing of anything may be done or evid notice or instrument;

Computer Misuse Act 1990

CHAPTER 18

ARRANGEMENT OF SECTIONS

Section

Computer misuse offences

1. Unauthorised access to computer material.
2. Unauthorised access with intent to commit or facilitate commission of further offences.
3. Unauthorised modification of computer material.

Jurisdiction

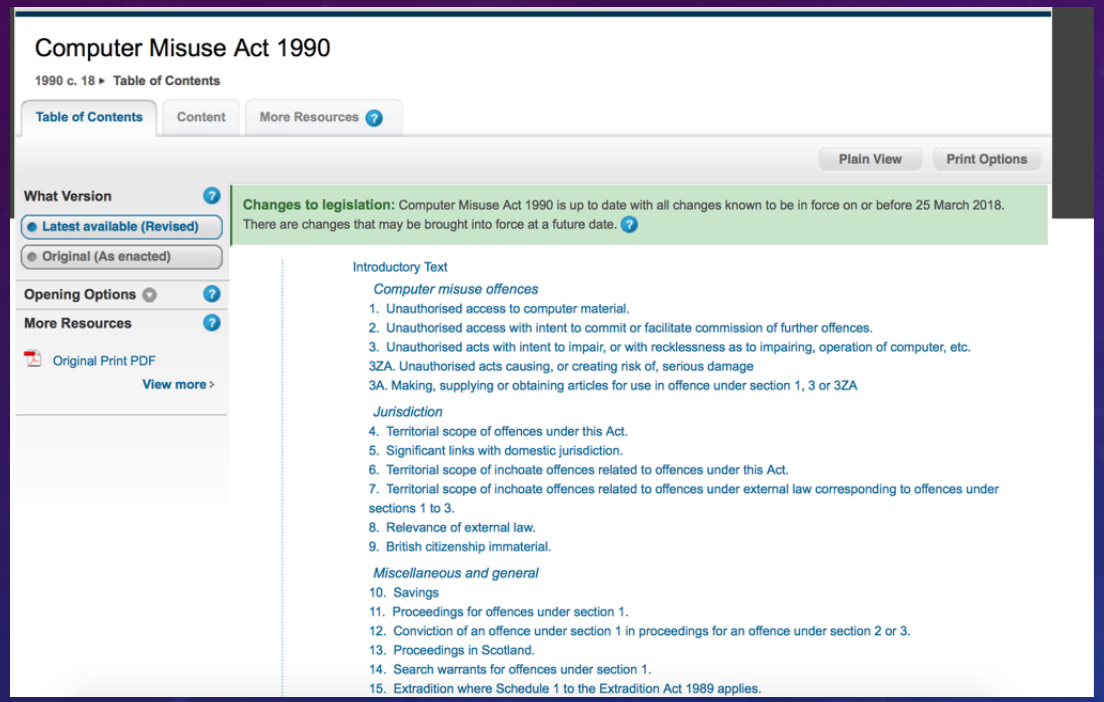
4. Territorial scope of offences under this Act.
5. Significant links with domestic jurisdiction.
6. Territorial scope of inchoate offences related to offences under this Act.
7. Territorial scope of inchoate offences related to offences under external law corresponding to offences under this Act.
8. Relevance of external law.
9. British citizenship immaterial.

Miscellaneous and general

10. Saving for certain law enforcement powers.
11. Proceedings for offences under section 1.
12. Conviction of an offence under section 1 in proceedings for an offence under section 2 or 3.
13. Proceedings in Scotland.
14. Search warrants for offences under section 1.
15. Extradition where Schedule 1 to the Extradition Act 1989 applies.
16. Application to Northern Ireland.
17. Interpretation.
18. Citation, commencement etc.

В Великобритании ответственность за компьютерные преступления установлена в статутах, принятых Парламентом. К основным актам, устанавливающим ответственность за компьютерные преступления, можно отнести: Закон о злоупотреблениях компьютерами 1990 г., Закон о телекоммуникациях (обмане) 1997 г., Закон о защите данных 1998 г., Закон об электронных коммуникациях 2000 г. и др.

ЗАКОНОДАТЕЛЬСТВО ВЕЛИКОБРИТАНИИ



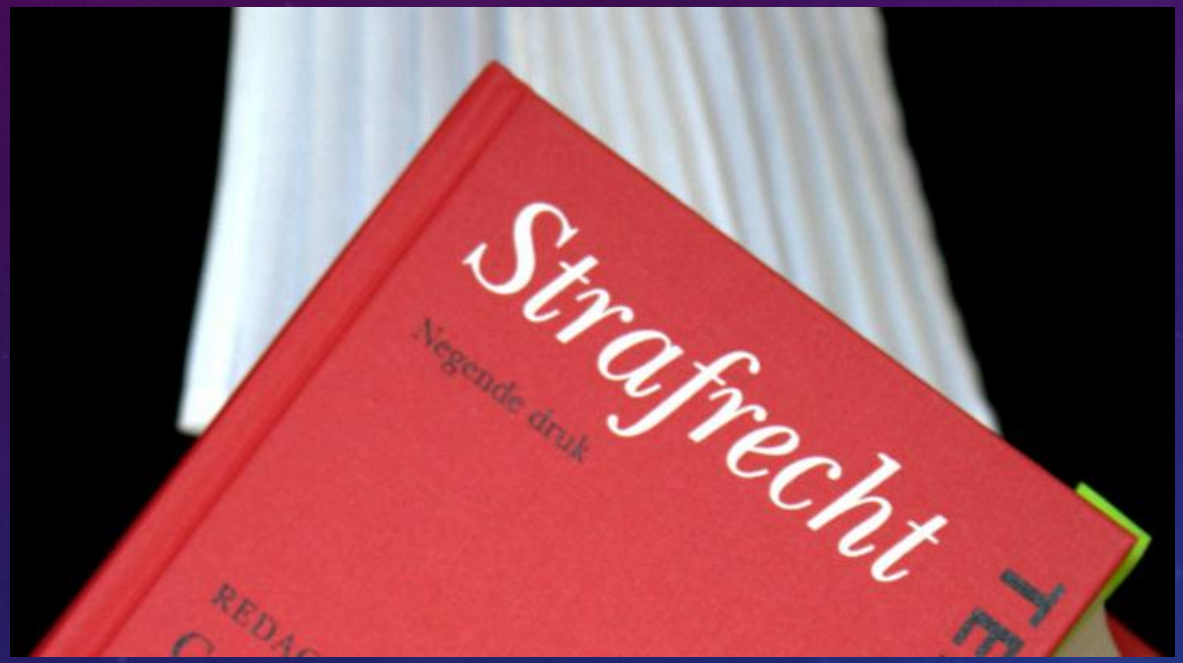
Первый параграф этого Акта о компьютерных злоупотреблениях касается "неуполномоченного доступа к компьютерным данным".

Им установлено, что лицо совершает преступление, когда оно использует компьютер для выполнения любой функции с намерением обеспечить доступ к любой программе или данным, содержащимся в любом компьютере, если этот доступ заведомо неправомочен.

ЗАКОНОДАТЕЛЬСТВО ВЕЛИКОБРИТАНИИ

В Великобритании ответственность за компьютерные преступления может наступить за распространение, использование и даже владение «инструментами взлома» т.е. инструментами используемыми для исследования безопасности.

ЗАКОНОДАТЕЛЬСТВО НИДЕРЛАНДОВ



Основным актом, касающимся компьютерной преступности в Нидерландах, является Закон об компьютерной преступности (Wet computercriminaliteit) 1993 года.

Это не отдельный акт, а закон, который входит в Уголовный кодекс Нидерландов (Wetboek van Strafrecht) и Уголовно-процессуальный кодекс (КПК) (Wetboek van Strafvordering)

ЗАКОНОДАТЕЛЬСТВО НИДЕРЛАНДОВ

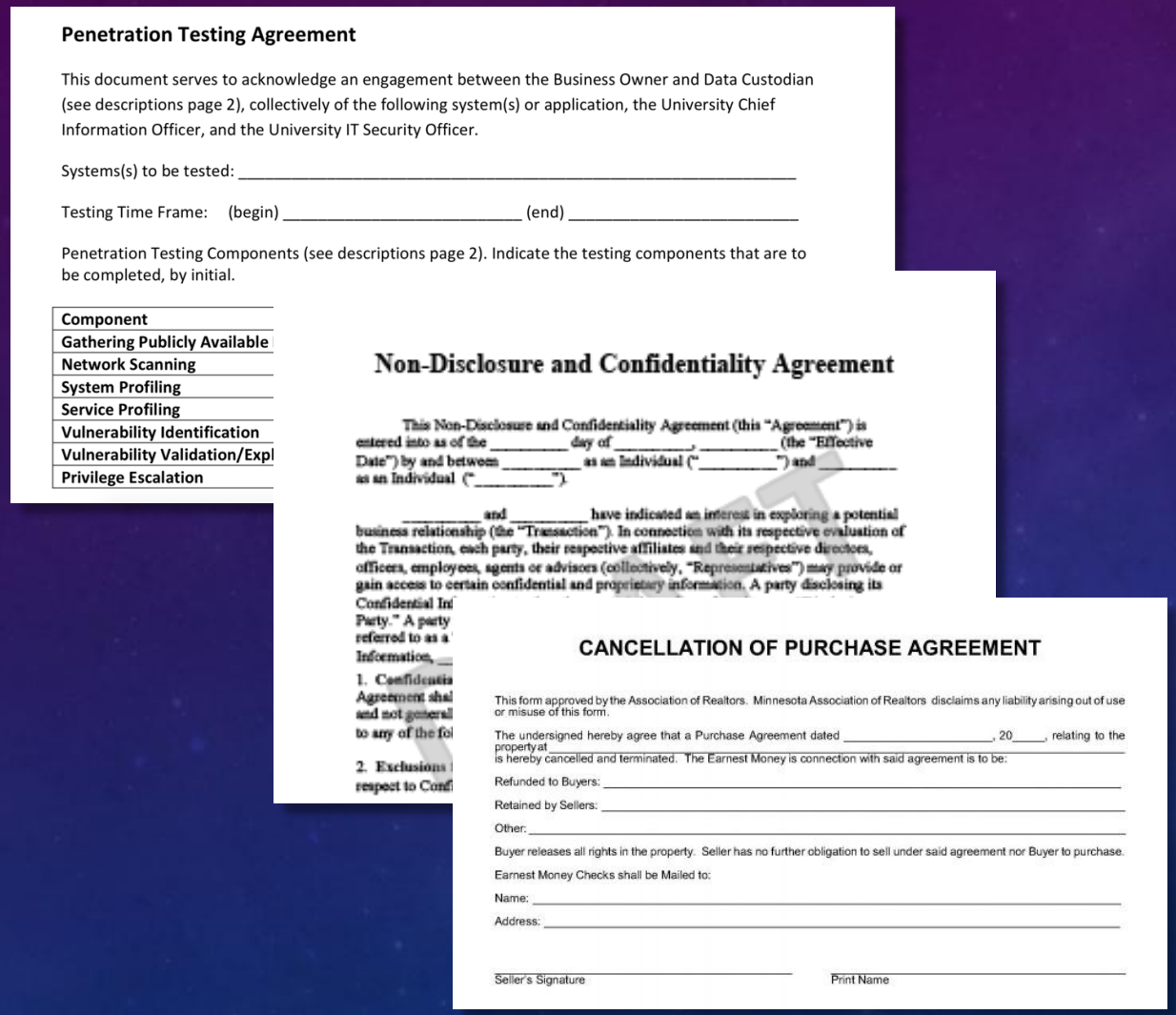
Согласно Уголовного кодекса Нидерландов компьютерным преступлением признается умышленное, … **использование лицом технических устройств** для перехвата или записи данных, идущих по телекоммуникационным системам или присоединенному оборудованию, если данные не предназначаются только для него(статья 139c УК). Лицо, снабжающее **средствами для незаконного перехвата и записи данных**, идущих по телекоммуникационным или автоматизированным системам, может быть подвергнуто наказанию – штрафу или заключению на срок до 6 месяцев (статья 139d).

Лицо, обладающее данными, о которых он знает или должен знать, что эти **данные были получены в результате незаконного прослушивания, записи или перехвата данн**ых автоматизированных систем или телекоммуникационных систем наказывается лишением свободы на срок до 6 месяцев (статья 139e)

ЗАКОНОДАТЕЛЬСТВО НИДЕРЛАНДОВ

Таким образом несанкционированный анализ или доступ к данным, идущим по телекоммуникационным системам или присоединенному оборудованию, а так же использование либо предоставление для использования средства для незаконного перехвата и записи данных в Голландии признается противозаконным

КАКОЙ ВЫХОД ?



Penetration Testing Agreement

This document serves to acknowledge an engagement between the Business Owner and Data Custodian (see descriptions page 2), collectively of the following system(s) or application, the University Chief Information Officer, and the University IT Security Officer.

Systems(s) to be tested: _____

Testing Time Frame: (begin) _____ (end) _____

Penetration Testing Components (see descriptions page 2). Indicate the testing components that are to be completed, by initial.

Component
Gathering Publicly Available
Network Scanning
System Profiling
Service Profiling
Vulnerability Identification
Vulnerability Validation/Expl
Privilege Escalation

Non-Disclosure and Confidentiality Agreement

This Non-Disclosure and Confidentiality Agreement (this "Agreement") is entered into as of the _____ day of _____, _____ (the "Effective Date") by and between _____ as an Individual ("_____") and _____ as an Individual ("_____").

_____ and _____ have indicated an interest in exploring a potential business relationship (the "Transaction"). In connection with its respective evaluation of the Transaction, each party, their respective affiliates and their respective directors, officers, employees, agents or advisors (collectively, "Representatives") may provide or gain access to certain confidential and proprietary information. A party disclosing its Confidential In
Party." A party
referred to as a
Information.
1. Confidentia
Agreement sha
and not general
to any of the fo
2. Exclusions
respect to Conf

CANCELLATION OF PURCHASE AGREEMENT

This form approved by the Association of Realtors. Minnesota Association of Realtors disclaims any liability arising out of use or misuse of this form.

The undersigned hereby agree that a Purchase Agreement dated _____, 20____, relating to the property at _____ is hereby cancelled and terminated. The Earnest Money is connection with said agreement is to be:

Refunded to Buyers: _____

Retained by Sellers: _____

Other: _____

Buyer releases all rights in the property. Seller has no further obligation to sell under said agreement nor Buyer to purchase.

Earnest Money Checks shall be Mailed to:

Name: _____

Address: _____

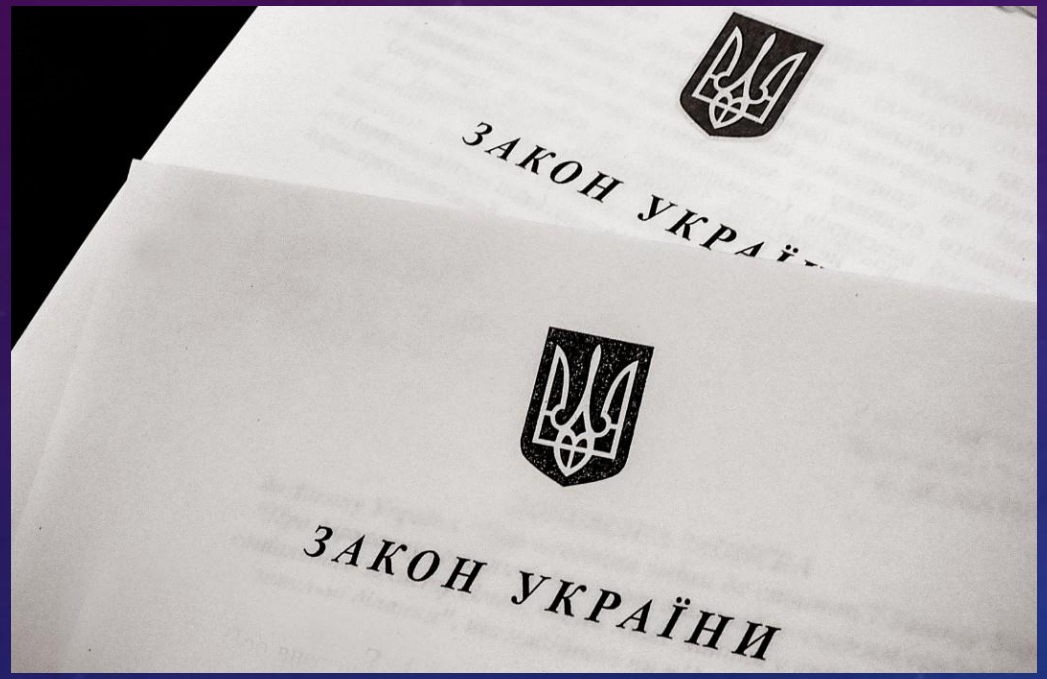
Seller's Signature

Print Name

- Договор о проведении пентеста Pent agreement
- Договор о неразглашении non-Disclosure agreement
- Договор об отказе от претензий Cancellation agreement

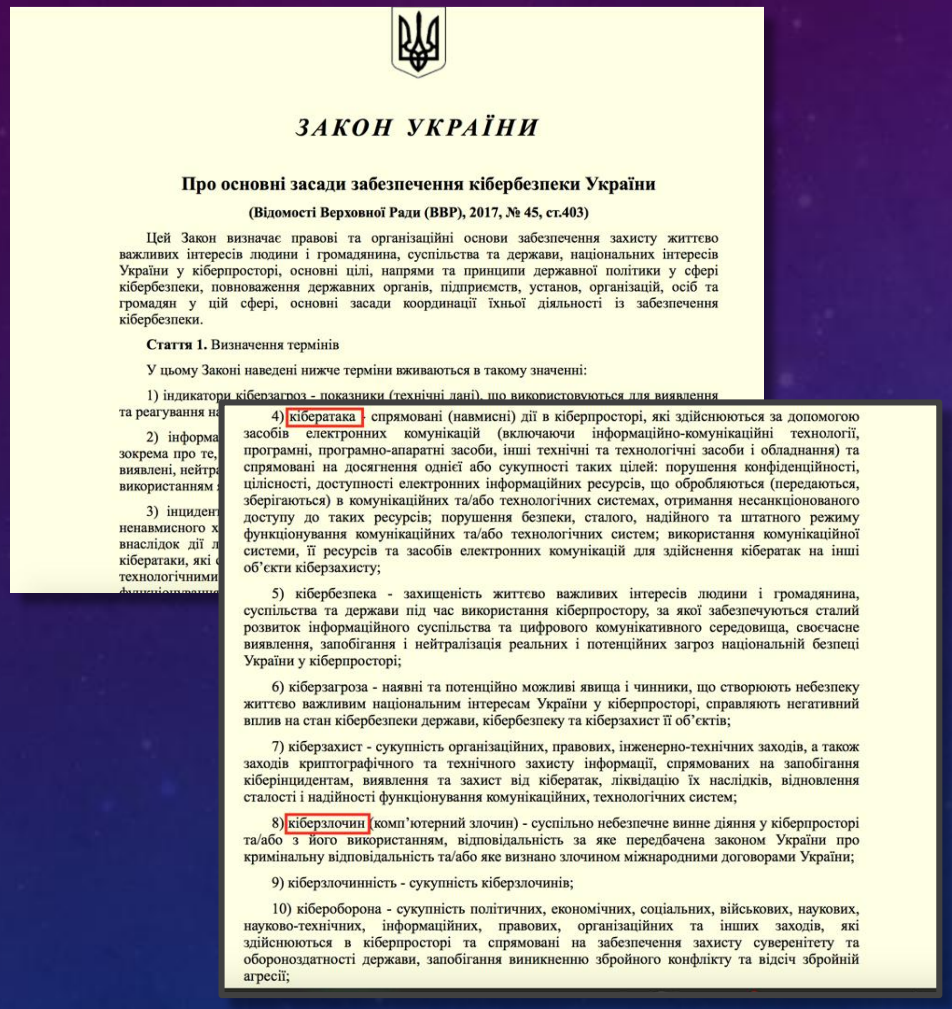
ТЕСТИРОВАНИЕ БЕЗОПАСНОСТИ В УКРАИНСКОМ ЗАКОНОДАТЕЛЬНО-ПРАВОВОМ ПОЛЕ

ЗАКОНОДАТЕЛЬСТВО УКРАИНЫ



- Уголовный кодекс Украины (раздел XVI)
- Закон Украины Об основных принципах обеспечения кибербезопасности Украины № 2163-VIII (вступает в силу 09.05.2018)

ЗАКОНОДАТЕЛЬСТВО УКРАИНЫ



ЗАКОН УКРАЇНИ

Про основні засади забезпечення кібербезпеки України

(Відомості Верховної Ради (ВВР), 2017, № 45, ст.403)

Цей Закон визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Стаття 1. Визначення термінів

У цьому Законі наведені нижче терміни вживаються в такому значенні:

1) індикатори кіберзагроз - показники (технічні дані), що використовуються для виявлення та реагування на

2) інформа зокрема про те, виявлені, нейтра використанням

3) інцидент ненавмисного х внаслідок дії л кібератаки, які технологічними

4) кібератака - спрямовані (навмисні) дії в кіберпросторі, які здійснюються за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) та спрямовані на досягнення однієї або сукупності таких цілей: порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, що обробляються (передаються, зберігаються) в комунікаційних та/або технологічних системах, отримання несанкціонованого доступу до таких ресурсів; порушення безпеки, сталого, надійного та штатного режиму функціонування комунікаційних та/або технологічних систем; використання комунікаційної системи, її ресурсів та засобів електронних комунікацій для здійснення кібератак на інші об'єкти кіберзахисту;

5) кібербезпека - захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі;

6) кіберзагроза - наявні та потенційно можливі явища і чинники, що створюють небезпеку життєво важливим національним інтересам України у кіберпросторі, справляють негативний вплив на стан кібербезпеки держави, кібербезпеку та кіберзахист її об'єктів;

7) кіберзахист - сукупність організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем;

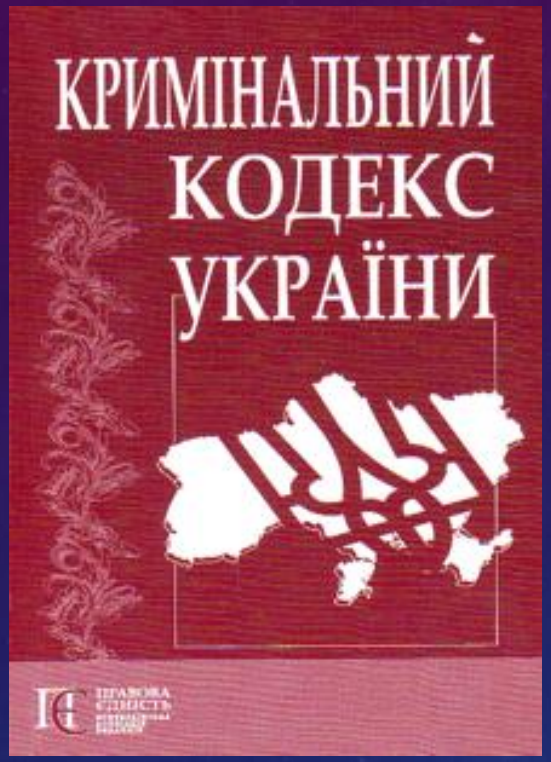
8) кіберзлочин (комп'ютерний злочин) - суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України;

9) кіберзлочинність - сукупність кіберзлочинів;

10) кібероборона - сукупність політичних, економічних, соціальних, військових, наукових, науково-технічних, інформаційних, правових, організаційних та інших заходів, які здійснюються в кіберпросторі та спрямовані на забезпечення захисту суверенітету та обороноздатності держави, запобігання виникненню збройного конфлікту та відсіч збройній агресії;

Закон Украины Об основных принципах обеспечения кибербезопасности Украины № 2163-VIII (вступает в силу 09.05.2018) призван унифицировать понятия используемые в сфере компьютерной безопасности и обеспечить правовую базу для построения систем защиты от киберугроз.

ЗАКОНОДАТЕЛЬСТВО УКРАИНЫ



Раздел 16 - Уголовного Кодекса Украины
Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи

Статья 361. Несанкционированное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи

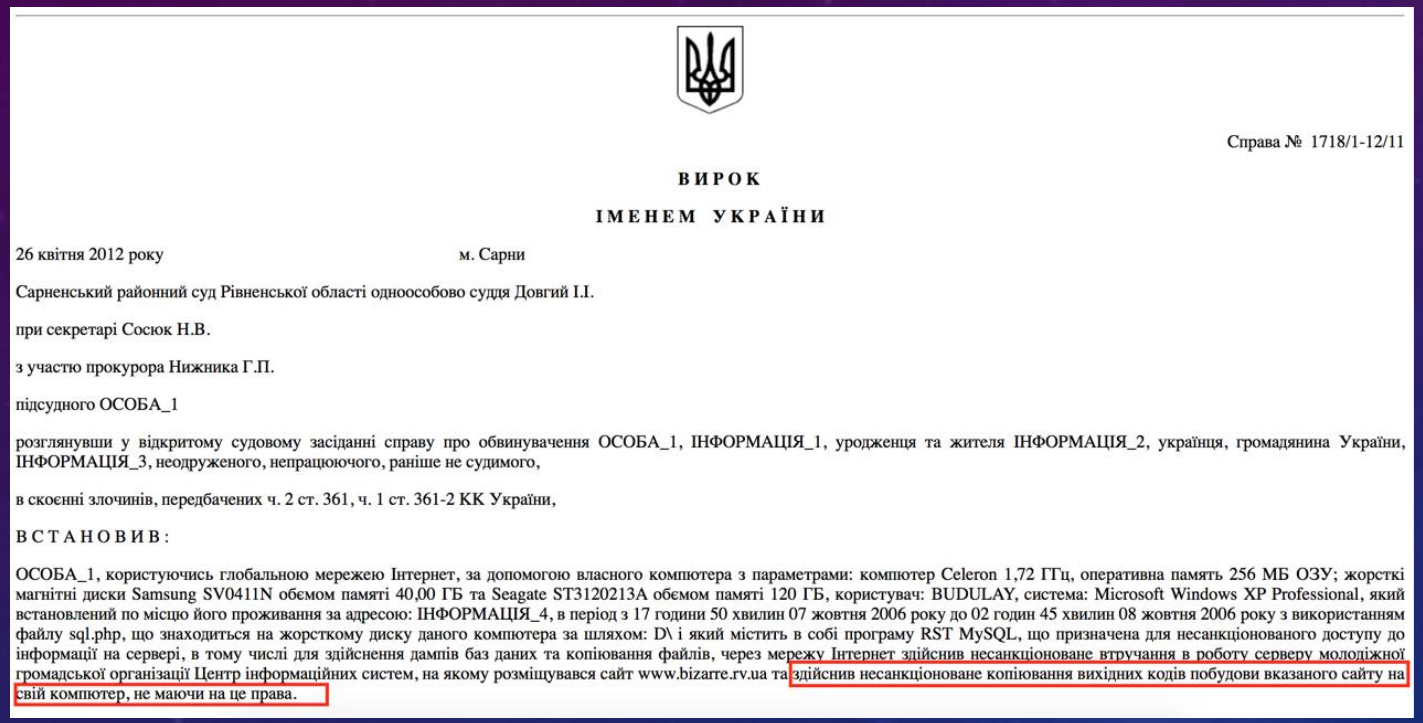
Статья 361-1. Создание с целью использования, распространения или сбыта вредных программных или технических средств, а также их распространение или сбыт

ЗАКОНОДАТЕЛЬСТВО УКРАИНЫ

Законодательство определяет, что несанкционирован-ное вмешательство в работу электронно-вычислительных машин (компьютеров), автоматизированных систем, компьютерных сетей или сетей электросвязи, что привело к утечке, потере, подделке, блокированию информации, искажению процесса обработки информации или к нарушению установленного порядка ее маршрутизации считается преступлением.

Незаконное вмешательство в работу ЭВМ, их систем или компьютерных сетей - это совершение определенных законом действий **без разрешения (согласия) соответствующего собственника или уполномоченных им лиц**, а так же влияние на работу АЭВМ с помощью различных технических устройств, способных повредить работе машины.

АНАЛИЗ СУДЕБНОЙ ПРАКТИКИ



Справа № 1718/1-12/11

ВИРОК

ІМЕНЕМ УКРАЇНИ

26 квітня 2012 року м. Сарни

Сарненський районний суд Рівненської області одноособово суддя Довгий І.І.

при секретарі Сосюк Н.В.

з участю прокурора Нижника Г.П.

підсудного ОСОБА_1

розглянувши у відкритому судовому засіданні справу про обвинувачення ОСОБА_1, ІНФОРМАЦІЯ_1, уродженця та жителя ІНФОРМАЦІЯ_2, українця, громадянина України, ІНФОРМАЦІЯ_3, неодруженого, непрацюючого, раніше не судимого,

в скоєнні злочинів, передбачених ч. 2 ст. 361, ч. 1 ст. 361-2 КК України,

ВСТАНОВИВ:

ОСОБА_1, користуючись глобальною мережею Інтернет, за допомогою власного компютера з параметрами: компютер Celeron 1,72 ГГц, оперативна память 256 МБ ОЗУ; жорсткі магнітні диски Samsung SV0411N обємом памяті 40,00 ГБ та Seagate ST3120213A обємом памяті 120 ГБ, користувач: BUDULAY, система: Microsoft Windows XP Professional, який встановлений по місцю його проживання за адресою: ІНФОРМАЦІЯ_4, в період з 17 години 50 хвилин 07 жовтня 2006 року до 02 годин 45 хвилин 08 жовтня 2006 року з використанням файлу sql.php, що знаходиться на жорсткому диску даного компютера за шляхом: D\ і який містить в собі програму RST MySQL, що призначена для несанкціонованого доступу до інформації на сервері, в тому числі для здійснення дампів баз даних та копіювання файлів, через мережу Інтернет здійснив несанкціоноване втручання в роботу серверу молодіжної громадської організації Центр інформаційних систем, на якому розміщувався сайт www.bizarre.rv.ua та здійснив несанкціоноване копіювання вихідних кодів побудови вказаного сайту на свій компютер, не маючи на це права.

Как пример применения 361 статьи Уголовного кодекса **Обвинительный** приговор суда за действия выразившиеся в несанкционированных сканировании web ресурса и копировании содержимого сайта

АНАЛИЗ СУДЕБНОЙ ПРАКТИКИ

Анализ применения судами Украины законодательства связанного с осуществлением несанкционированного доступа к хостам и сетям (ст. 361 КК)

Теми действиями которые формально подпадают под способы и методы проведения анализа состояния безопасности компьютерных систем

Выявлено преступлений (данные МВД) по 361 УК Украины – 3527

Приговор по 361 УК Украины – 22

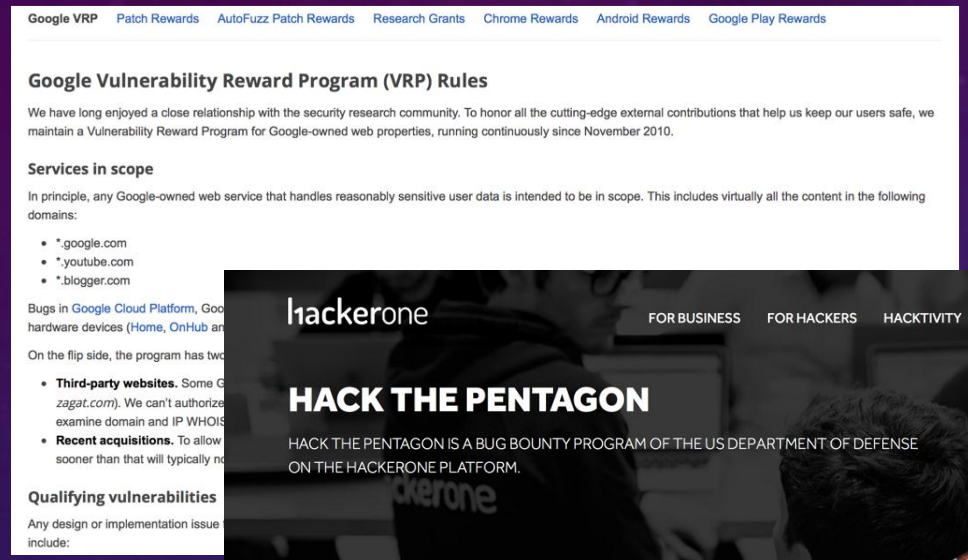
Приговоры за «тестирование безопасности» - 0

BUG BOUNTY ПОИСК БАГОВ ЗА ВОЗНАГРАЖДЕНИЕ

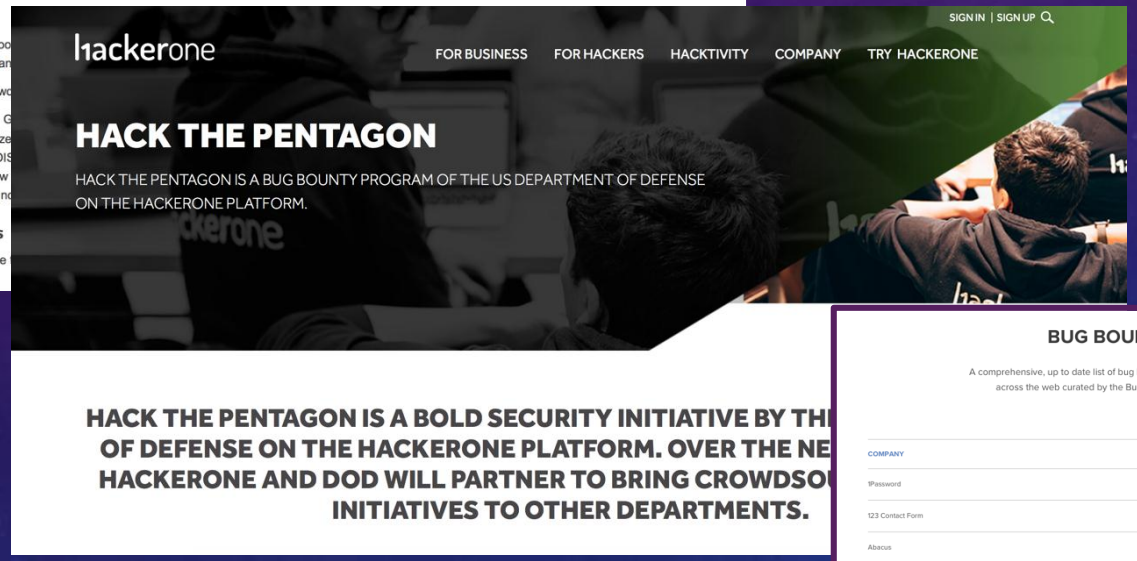
Одна из самых эффективных мер в сфере безопасности (IT Security) — программа поиска и выявления уязвимостей (bug bounty).

Большинство компаний представлено на площадках — агрегаторах, таких как HackerOne или BugCrowd.
Многие компании открыли как собственные программы, так и профили на HackerOne. Это все мировые IT гиганты.
Даже у Пентагона есть своя программа BugBounty.
Средняя сумма выплат составляет от $200 до $1000, в зависимости от уязвимости и места ее нахождения.

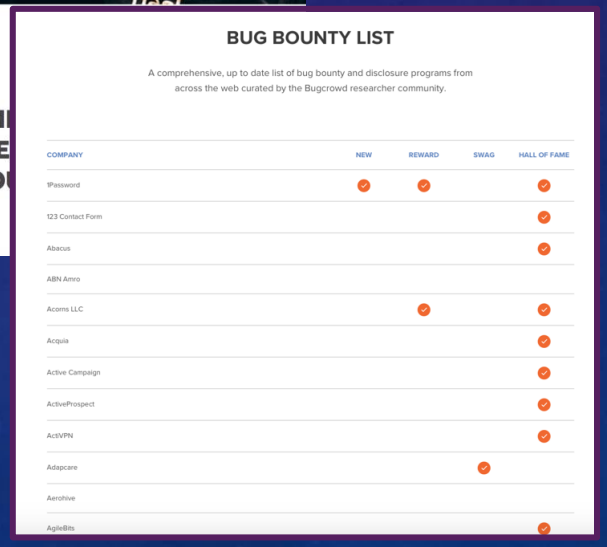
BUG BOUNTY ПОИСК БАГОВ ЗА ВОЗНАГРАЖДЕНИЕ



Bug Bounty от GOOGLE



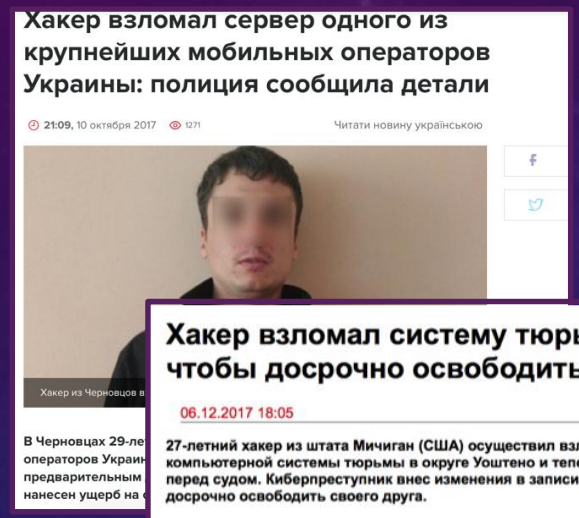
Bug Bounty Пентагона



Агрегатор Bug Bounty программ BugCrowd

УЯЗВИМОСТЬ ЕСТЬ - BUG BOUNTY НЕТ

black hat hacker

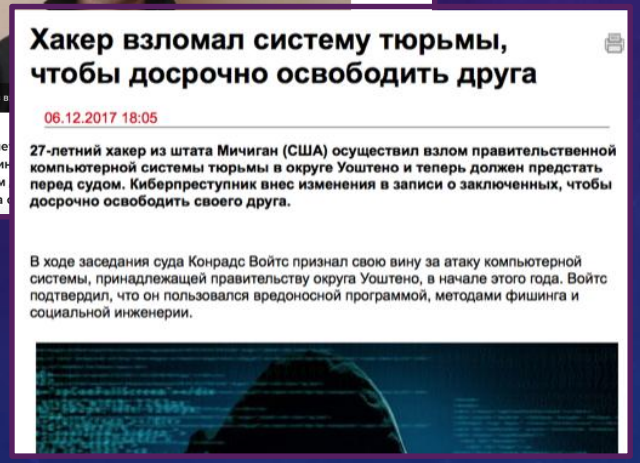


Хакер взломал сервер одного из крупнейших мобильных операторов Украины: полиция сообщила детали

21:09, 10 октября 2017 1271 Читати новину українською

Хакер из Черновцов в

В Черновцах 29-ле
операторов Украин
предварительным
нанесен ущерб на



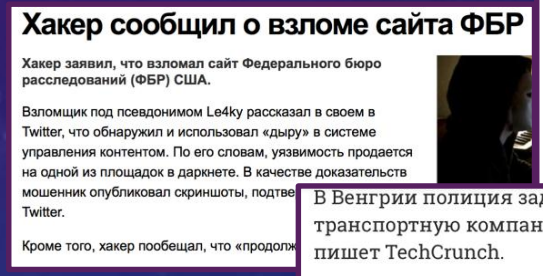
Хакер взломал систему тюрьмы, чтобы досрочно освободить друга

06.12.2017 18:05

27-летний хакер из штата Мичиган (США) осуществил взлом правительственной компьютерной системы тюрьмы в округе Уоштено и теперь должен предстать перед судом. Киберпреступник внес изменения в записи о заключенных, чтобы досрочно освободить своего друга.

В ходе заседания суда Конрадс Войтс признал свою вину за атаку компьютерной системы, принадлежащей правительству округа Уоштено, в начале этого года. Войтс подтвердил, что он пользовался вредоносной программой, методами фишинга и социальной инженерии.

white hat hacker

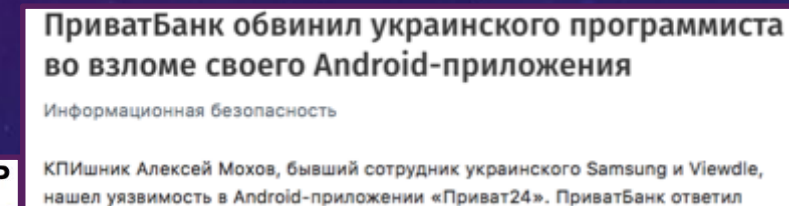


Хакер сообщил о взломе сайта ФБР

Хакер заявил, что взломал сайт Федерального бюро расследований (ФБР) США.

Взломщик под псевдонимом Le4ky рассказал в своем в Twitter, что обнаружил и использовал «дыру» в системе управления контентом. По его словам, уязвимость продается на одной из площадок в даркнете. В качестве доказательств мошенник опубликовал скриншоты, подтве
Twitter.

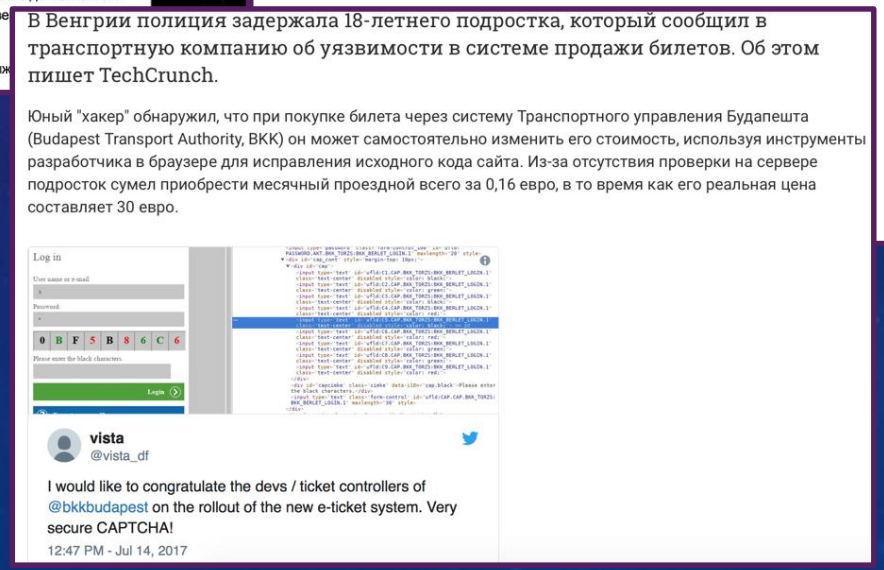
Кроме того, хакер пообещал, что «продолж



ПриватБанк обвинил украинского программиста во взломе своего Android-приложения

Информационная безопасность

КПИшник Алексей Мохов, бывший сотрудник украинского Samsung и Viewdle, нашел уязвимость в Android-приложении «Приват24». ПриватБанк ответил неожиданно, обвинив программиста в попытке украсть средства со счетов клиентов банка.



В Венгрии полиция задержала 18-летнего подростка, который сообщил в транспортную компанию об уязвимости в системе продажи билетов. Об этом пишет TechCrunch.

Юный "хакер" обнаружил, что при покупке билета через систему Транспортного управления Будапешта (Budapest Transport Authority, BKK) он может самостоятельно изменить его стоимость, используя инструменты разработчика в браузере для исправления исходного кода сайта. Из-за отсутствия проверки на сервере подросток сумел приобрести месячный проездной всего за 0,16 евро, в то время как его реальная цена составляет 30 евро.

Log in

0 B F 5 B 8 6 C 6

Please enter the black characters.

Login

vista
@vista_df

I would like to congratulate the devs / ticket controllers of @bkkbudapest on the rollout of the new e-ticket system. Very secure CAPTCHA!

12:47 PM - Jul 14, 2017

СО СТОРОНЫ ЗАКОНА

black hat hacker

=

white hat hacker

#FuckResponsibleDisclosure

#FuckResponsibleDisclosure - флешмоб IT-фахівців з UCA змушує українські держструктури дбати про інформаційну безпеку - Info

INFORMNAPALM.ORG

InformNapalm Україна
11 декабря 2017 г. ·

Кібербезпека стала в Україні не менш модною темою, ніж боротьба з корупцією. Український кіберальянс і незалежні дослідники кілька тижнів шукали вразливі системи в державному секторі. Настав час підбити підсумки флешмобу #FuckResponsibleDisclosure
https://informnapalm.org/.../aktyvisty-pidbyly-pidsumky-fles.../

Активісти підбили підсумки флешмобу #FuckResponsibleDisclosure з виявлення вразливостей державних IT-систем України -...

INFORMNAPALM.ORG

#FuckResponsibleDisclosure это сетевой флешмоб:
Хактивисты были настолько опечалены безразличной и легкомысленной реакцией организаций на выявленные проблемы безопасности, что прибегли к публичной публикации данных об опасности, разгласив полную информацию о найденных уязвимостях.

Sean Brian Townsend
около 4 месяцев назад

САБОТАЖ (Сетевой диск киевской полиции в открытом доступе)
(буду благодарен за репост)

Буквально на днях в Твиттере проснулся спящий аккаунт "Anonymous Poland" (на самом деле Russia) и запостил подборку личных данных участников АТО, волонтёров, телефонные справочники чиновников Черниговской области. Не прошло и нескольких суток, как Департамент кіберполіції Національної поліції України нашел компьютер, с которого произошла утечка. Я сомневаюсь в том, что у них получится найти... See More

```
 //195.230.144.11/
an's password:
Ultimate 7601 Service Pack 1] Server=[Windows 7

ame       Type      Comment
---       ----      -------
          Disk      Удаленный Admin
          Disk      Стандартный общий ресурс
MF3200 Series Printer   Canon MF3200 Series
          Disk      Стандартный общий ресурс
          IPC       Удаленный IPC
Marina    Disk
          Disk      Драйверы принтеров
          Disk
кументы   Disk
```

ВЫВОД

ТЕСТИРОВАНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Должно осуществляться в рамках соответствующих программ по типу BUG BOUNTY или только после подписания договоров предусматривающих взаимные обязательства и отказ от претензий.

Иное может быть признано незаконным.

СОВРЕМЕННЫЕ ПРАВОВЫЕ РЕШЕНИЯ

SUPRI.PRO
facebook.com/www.supri.pro/

facebook.com/0leg.d
linkedin.com/in/oleg-d-a735a772/

СПАСИБО ЗА ВНИМАНИЕ