БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

УТВЕРЖДАЮ
Проректор по учебной работе и образовательным инновациям
_____ О.И. Чуприс
«25» ноября 2019 г.
Регистрационный № УД-7423 /уч.

Международно-правовые основы информационной безопасности

(на английском языке)
Учебная программа учреждения высшего образования по факультативной дисциплине для специальности:

1-24 01 02 Правоведение
1-24 01 03 Экономическое право

2019 г.

Учебная программа составлена на основе ОСВО 1-24 01 02-2013, 1-24 01 03-2013 и учебных планов от 30.05.2013 г. рег.№ Е24-175/уч., рег. № Е24-174/уч., рег. № Е24и-230/уч., рег. № Е24и-231/уч.

СОСТАВИТЕЛИ:
Н.О. Мороз – доцент кафедры государственного управления юридического факультета Белорусского государственного университета, кандидат юридических наук, доцент.

РЕЦЕНЗЕНТЫ:
А.С. Бакун – доцент кафедры конституционного права Академии управления при Президенте Республики Беларусь, кандидат юридических наук, доцент

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ:
Кафедрой государственного управления юридического факультета Белорусского государственного университета
«17» октября 2019 г., протокол № 3;

Учебно-методической комиссией юридического факультета Белорусского государственного университета «15» ноября 2019 г., протокол № 3.

Заведующий кафедрой _____ Т.А. Червякова

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная программа по факультативной дисциплине ***«Международно-правовые основы информационной безопасности»*** разработана для обучающихся на первой ступени высшего образования дневной формы получения высшего образования специальности 1-24 01 02 «Правоведение».

Цели и задачи учебной дисциплины.

Целью изучения факультативной дисциплины «Международно-правовые основы информационной безопасности» являются: получение знаний по теоретико-правовым, институционным и договорным основам сотрудничества в обеспечении информационной безопасности, а также выработка у обучающихся умений по применению в практической деятельности полученных знаний по учебной дисциплине.

Задачами факультативной дисциплины «Международно-правовые основы информационной безопасности» являются*:*

– формирование знаний о системе норм и принципов, регулирующих вопросы международной информационной безопасности;

– приобретение знаний в области правовых форм организации и осуществления международного сотрудничества в борьбе с преступностью в сфере высоких технологий;

– формирование навыков работы с международными договорами, актами органов международных организаций, решениями международных судов, нормативно-правовыми актами.

Место дисциплины в системе подготовки специалистов.

Дисциплина относится к циклу ***факультативных дисциплин (компонент учреждения высшего образования).***Факультативная дисциплина «Международно-правовые основы информационной безопасности» включает систематизированное изложение теоретических вопросов, раскрывающих сущность информационной безопасности, а также особенности противодействие военно-политическим угрозам в информационное сфере, деструктивному информационному воздействию и преступности в сфере высоких технологий, а также выявление роли международных организаций в области обеспечения международной информационной безопасности, что позволит обучающимся в практической деятельности успешно решать конкретные задачи, стоящие перед Республикой Беларусь, в сфере обеспечения национальной информационной безопасности. Дисциплина преподается на английском языке.

Связи с другими учебными дисциплинами выражается в том, что преподавание учебной дисциплины базируется на предварительном изучении такой дисциплины как «Международное публичное право».

Требования к компетенциям. Освоение факультативной дисциплины «Международно-правовые основы информационной безопасности» должно обеспечить формирование следующих академических, социально-личностных и профессиональных компетенций:

Академические компетенции (АК):

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным вырабатывать новые идеи (обладать креативностью).

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

АК-8. Обладать навыками устной и письменной коммуникации.

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

Социально-личностные компетенции (СЛК):

СЛК-1. Обладать качествами гражданственности.

СЛК-2. Быть способным к социальному взаимодействию.

СЛК-3. Обладать способностью к межличностным коммуникациям.

СЛК-5. Быть способным к критике и самокритике.

СЛК-6. Уметь работать в команде.

СЛК-7. Выполнять требования правовых актов в профессиональной и других сферах своей жизнедеятельности.

СЛК-8. Соблюдать правила профессиональной этики.

Профессиональные компетенции (ПК):

ПК-1. Защищать гарантированные Конституцией Республики Беларусь и иными законодательными актами личные права и свободы, социально-экономические и политические права граждан, конституционный строй Республики Беларусь, государственные и общественные интересы.

ПК-22. Давать консультации и разъяснения по юридическим вопросам.

ПК-23. Составлять заявления, жалобы и другие документы правового характера.

ПК-24. Представлять интересы клиентов в судах.

ПК-27. Проводить правовую оценку документов и деятельности.

ПК-30. Организовывать правовое обеспечение работы государственного органа, предприятия, организации, учреждения.

ПК-31. Обеспечивать законность в деятельности государственного органа, предприятия, организации, учреждения.

ПК-37. Консультировать по правовым вопросам, возникающим в деятельности государственного органа, предприятия, организации, учреждения.

ПК-70. Готовить доклады, материалы к презентациям.

ПК-71. Пользоваться глобальными информационными ресурсами.

ПК-72. Владеть современными средствами телекоммуникаций.

ПК-73. Преподавать юридические и экономические дисциплины на современном научно-теоретическом и методическом уровнях в учреждениях общего среднего и среднего специального образования.

В результате изучения учебной дисциплины студент должен

знать:

– основные теоретико-методологические основы международной информационной безопасности;

– систему международных организаций, координирующих международное сотрудничество государств в сфере обеспечения международной информационной безопасности;

– формы и направления сотрудничества государств в борьбе с преступностью в сфере высоких технологий;

уметь:

– характеризовать систему и содержание правовых отношений в сфере международного сотрудничества в сфере обеспечения информационной безопасности;

– анализировать особенности международно-правовых отношений в борьбе с преступностью в сфере высоких технологий в условиях глобализации;

– работать с международными договорами, актами органов международных организаций, решениями международных судов и трибуналов, нормативно-правовыми актами в сфере обеспечения международной информационной безопасности;

владеть:

– основными способами применения норм международных документов в сфере обеспечения международной информационной безопасности;

– методами правовой квалификации фактов, событий и действий;

– правовой терминологией в сфере международного сотрудничества по обеспечению информационной безопасности.

Дисциплина преподается на английском языке.

Структура учебной дисциплины.

Дисциплина изучается в 4 семестре. Всего на изучение учебной дисциплины «Международно-правовые основы информационной безопасности (на английском языке» отведено:

– для очной формы получения высшего образования– 24 часов, в том числе 24 аудиторных часов, из них: лекции – 10 часов, семинарские занятия – 14часов.

Трудоемкость учебной дисциплины составляет 0,5 зачетные единицы.

Форма текущей аттестации – зачет.

СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

TOPIC 1. THEORETICAL FRAMEWORK FOR INFORMATION SECURITY

The concept of information security. Definition of cyber-terms (computer security, cyber security, information security.

Features of international information security (subjects and objects). Types of information security. Information security threats. Jurisdiction in cyberspace. State cyber neutrality. Direct and indirect attribution in cyberspace. Western and eastern legal approach to ensuring information security. International legal cooperation in ensuring information security.

The place of principles and norms regulating the issues of international information security in the system of international law.

TOPIC 2. THREATS TO INFORMATION SECURITY

Notion of cyber attack. Types of cyber attacks. Cyber attack as a use of force.

Countering military-political threats in the field of international information security. Interference in internal affairs through information and telecommunication technologies (ICTs). Violation of sovereignty by means of cyber technologies. Unfriendly acts in cyberspace. Destructive information influence and international law. The use of information infrastructure for the dissemination of information inciting ethnic, interracial and interfaith enmity. Manipulation of information flows in the information space of other states, misinformation and concealment of information in order to distort the psychological and spiritual environment of society.

Information warfare, information weapons and international law. Cyberattack and cybergression. International law applicable to hostilities in cyberspace. Cyber attacks in the course of war.

State response against cyber attacks carried out by state actors (self-defense, countermeasures, retortion). Cybercrime. Obligation *aut dedere aut judicare*. State liability for actions of private individuals. Applicability of due diligence principle to cyberspace.

TOPIC 3. INTERNATIONAL LEGAL FRAMEWORK FOR INFORMATION SECURITY

International legal regulation for international information security at universal level. Regional treaties regulating the cooperation of states in the field of information security. Bilateral international treaties in the field of information security. Draft Convention on International Information Security, proposed by Russian Federation. Prospects for international cooperation in the field of international information security.

The role of soft law in regulating the provision of international information security (norms of responsible state behavior in cyberspace).

Information security and human rights. Applicability of human rights conventions to actions in cyber space. Core human rights and cyber technologies. Freedom of expression, right to privacy and ensuring information security. Mass surveillance

and human rights law. Fake news, propaganda, incitement to crime and human rights law.

TOPIC 4. ROLE OF INTERNATIONAL ORGANIZATIONS IN ENSURING INTERNATIONAL INFORMATION SECURITY

The role of the UN in coordinating international cooperation in the field of international information security. The activities of the UN General Assembly, the UN Security Council in the field of international information security. The mandate of the UN Group of Governmental Experts (GGE) on Advancing responsible State behaviour in cyberspace in the context of international security; Open-Ended Working Group on Developments in the Field of ICTs in the Context of International Security.

The activities of regional international organizations in the field of information security (NATO, CSTO, CIS, SCO). Tallinn Manual on the Law Applicable to Cyber Warfare. The initiative of the SCO member states in the field of responsible state behavior in cyberspace.

Legal framework for ensuring cyber security in the EU.

TOPIC 5. INTERNATIONAL LEGAL COOPERATION IN THE FIGHT AGAINST CYBERCRIME

International legal cooperation in the fight against cybercrime at universal and regional level. Forms and directions of international legal cooperation in the fight against cybercrime. International legal regulation of state cooperation in the fight against cybercrime.

International legal cooperation in the fight against cybercrime within the framework of international organizations (UN, Interpol, CIS, Council of Europe, European Union, Organization of American States, CSTO).

УЧЕБНО-МЕТОДИЧЕСКАЯ КАРТА УЧЕБНОЙ ДИСЦИПЛИНЫ

Дневная форма получения высшего образования

Номер раздела, темы	Название раздела, темы	Количество аудиторных часов					Количество часов УСР	Форма контроля знаний
		Лекции	Практические занятия	Семинарские занятия	Лабораторные занятия	Иное		
1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*
1.	Theoretical framework for information security	2		2				Discussion, case study
2.	Threats to information security	4		6				Discussion, case study
3.	International legal framework for information security	2		2				Test
4.	Role of international organizations in ensuring international information security			2				Essay
5.	International legal cooperation in the fight against cybercrime	2		2				Discussion, case study
	Total	10		14				

ИНФОРМАЦИОННО-МЕТОДИЧЕСКАЯ ЧАСТЬ

Перечень основной литературы

1. Довгань Е.Ф. Международные организации и поддержание международного мира и безопасности : моногр. / Е.Ф. Довгань. – Минск : Междунар. ун-т «МИТСО», 2016. – 262 с.

2. Мороз, Н.О. Роль ООН в обеспечении информационной безопасности / Н.О. Мороз // «70 лет Организации Объединенных Наций (1945-2015 гг.). Мой мир: повестка дня устойчивого развития после 2015 г.» : сб. ст. науч.-практ. конф. молод. учен., Минск, 27 мая 2015 г. / под ред. Е.Ф. Довгань. – Минск : Междунар. ун-т «МИТСО», 2015. – С. 82–92.

3. Мороз, Н.О. Международно-правовые основы обеспечения международной информационной безопасности / Н.О. Мороз // Труд. Профсоюзы. Общество. – 2016. – № 1 (51). – С. 77–81.

4. Мороз, Н.О. Договорно-правовая деятельность в борьбе с преступностью в сфере высоких технологий / Н.О. Мороз // Право.by. – 2010. – № 1. – С. 41–47.

Перечень дополнительной литературы

5. Довгань Е.Ф. ОДКБ и информационная безопасность / Е.Ф. Довгань, Н.О. Мороз // Организация Договора о коллективной безопасности и планирование на случай чрезвычайных обстоятельств после 2014 г. / Н.О. Мороз [и др.] ; под ред. Е.Ф. Довгань и А.В. Русаковича; Женевский центр демократического контроля над вооруженными силами, Центр изучения внешней политики и безопасности. – Женева – Минск, 2015. – С. 207–236.

6. Feasibility study for a European Cybercrime Centre [Electronic resource] : final rep. / N. Robinson [et al.] ; RAND Europe. – 2012. – Mode of access : http://ec.europa.eu/home-affairs/doc_centre/crime/docs/20120311_final_report_feasibility_study_for_a_european_cybercrime_centre.pdf. – Date of access : 10.07.2014.

7. Global Cybersecurity Agenda // International Telecommunication Union [Electronic resource]. – Mode of access : http://www.itu.int/osg/csd/cybersecurity/gca/index.html. – Date of access : 12.02.2013.

8. Handler, S.G. The new cyber face of battle: developing a legal approach to accommodate emerging trends in warfare / S.G. Handler // Stanford J. of Intern. Law. – 2012. – Vol. 48, № 1. – P. 209–237.

9. International multi-lateral partnership against cyber terrorism // International Telecommunication Union [Electronic resource]. – Mode of access : http://www.itu.int/ITU-D/cyb/publications/2012/IMPACT/IMPACT-en.pdf. – Date of access : 11.10.2012.

10. Internet and the law : recommendation 1670 (2004)1 of Parliamentary Assembly, 7 Sept. 2004 // Council of Europe [Electronic

resource]. – Mode of access : http://assembly.coe.int/main.asp?Link=/documents/adoptedtext/ta04/erec1670.htm. – Date of access : 11.11.2012.

11. Lloyd, I.J. Information technology law / I.J. Lloyd. – New York : Oxford Univ. Press, 2011. – 597 p.

12. NATO and cyber defence // North Atlantic Treaty Organization [Electronic resource]. – Mode of access : http://www.nato.int/cps/en/SID-A7190628-8FCC66CD/natolive/topics_78170.htm. – Date of access : 13.10.2012.

13. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience : communication from the Commiss. to the Europ. Parliament, the Council, the Europ. Econ. a. Social Comm. a. the Comm. of the Regions on Crit. Inform. Infrastructure Protection, Brussels, 30 March 2009, COM(2009) 149 final // EUR-Lex.europa.eu [Electronic resource]. – Mode of access : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:EN:HTML. – Date of access : 01.06.2012.

14. Sofaer, A.D. Cyber crime and security / A.D. Sofaer // Transnational dimension of cybercrime and terrorism / A.D. Sofaer [et al.]. – Stanford, 2001. – P. 1–34.

15. The EU Internal Security Strategy in Action: five steps towards a more secure Europe : communication from the Commiss. to the Europ. Parliament a. the Council, Brussels, 22 Nov. 2010, COM(2010) 673 final // EUR-Lex.europa.eu [Electronic resource]. – Mode of access : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0673:FIN:EN:PDF. – Date of access : 01.06.2012.

16. Towards a general policy on the fight against cyber crime : communication from the Commiss. to the Europ. Parliament, the Council a. the Comm. of the Regions, Brussels, 22 May 2007, COM(2007) 267 final // EUR-Lex.europa.eu [Electronic resource]. – Mode of access : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2007:0267:FIN:EN:PDF. – Date of access : 01.06.2012.

17. Zekos, G.I. Cyber-territory and jurisdiction of Nations / G.I. Zekos // J. of Internet Law. – 2012. – Vol. 15, № 12. – P. 3–23.

Нормативно-правовые акты

18. Конституция Республики Беларусь 1994 года (с изменениями и дополнениями, принятыми на республиканских референдумах 24 ноября 1996 г. и 17 октября 2004 г.). – Минск : Амалфея, 2013. – 48 с.

19. О международных договорах Республики Беларусь : Закон Респ. Беларусь, 23 июля 2008 г., № 421-З : в ред. Закона Респ. Беларусь от 8.01.2014 г. // Консультант Плюс : Беларусь. Технология 3000

[Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2015.

20. Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 : в ред. Указа Президента Респ. Беларусь от 24.01.2014 г. // Консультант Плюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2015.

21. Уголовно-процессуальный кодекс Республики Беларусь : Кодекс Респ. Беларусь, 16 июля 1999 г., № 295-З : принят Палатой представителей 24 июня 1999 г. : одобр. Советом Респ. 30 июня 1999 г. : в ред. Закона Респ. Беларусь от 10.01.2015 г. // Консультант Плюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – М., 2015.

Международные договоры и
акты органов международных организаций

22. Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems : [Strasbourg, 21.01.2003] // Council of Europe [Electronic resource]. – Mode of access : http://conventions.coe.int/Treaty/en/Treaties/html/189.htm. – Date of access : 22.10.2012.

23. Arab Convention on Combating information technology offences, 21 December 2010 [Electronic resource] / League of Arab States, Gen. Secretariat. – Mode of access : https://www.google.by/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&sqi=2&ved=0CCsQFjAA&url=https%3A%2F%2Fcms.unov.org%2FDocumentRepositoryIndexer%2FGetDocInOriginalFormat.drsx%3FDocID%3D3dbe778b-7b3a-4af0-95ce-a8bbd1ecd6dd&ei=Kmp5Uer1EMPQtQbqtoHwDw&usg=AFQjCNHqL8HCKiOheQwiqkViDzhK5dtOpQ&bvm=bv.45645796,d.Yms. – Date of access : 02.04.2013.

24. Convention on cybercrime, Budapest, 23 November 2001 // Council of Europe [Electronic resource]. – Mode of access : http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm. – Date of access : 22.10.2012.

25. Council Recommendation of 25 June 2001 on contact points maintaining a 24-hour service for combating high-tech crime, 2001/C 187/02 // EUR-Lex.europa.eu [Electronic resource]. – Mode of access : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2001:187:0005:0006:EN:PDF. – Date of access : 14.02.2013.

26. Council Resolution of 18 December 2009 on a collaborative European approach to Network and Information Security, 2009/C 321/01 // EUR-Lex.europa.eu [Electronic resource]. – Mode of access : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:01:EN:HTML. – Date of access : 14.02.2013.

27. Council Resolution of 18 February 2003 on a European approach towards a culture of network and information security, 2003/C 48/01 // EUR-Lex.europa.eu [Electronic resource]. – Mode of access : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32003G0228(01):EN:HTML. – Date of access : 14.02.2013.

28. Creating a safer information society by improving the security of information infrastructures and combating computer-related crime : communication from the Commiss. to the Council, the Europ. Parliament, the Econ. a. Social Comm. a. the Comm. of the Regions, Brussels, 26 Jan. 2001, COM (2000) 890 final // EUR-Lex.europa.eu [Electronic resource]. – Mode of access : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0890:FIN:EN:PDF. – Date of access : 01.06.2012.

29. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA // EUR-Lex.europa.eu [Electronic resource]. – Mode of access : http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF. – Date of access : 14.10.2013.

30. Конвенция Организации Объединенных Наций против транснациональной организованной преступности : [принята в г. Нью-Йорке 15.11.2000 г.] // Международное право и борьба с преступностью : сб. док. / Моск. гос. ин-т междунар. отношений (ун-т) ; сост.: А.В. Змеевский, Ю.М. Колосов, Н.В. Прокофьев. – М., 2004. – С. 433–478.

31. Конвенция СНГ о правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам : [совершено в г. Кишиневе 07.10.2002 г.] // Содружество. – 2002. – № 2. – С. 82–130.

32. Соглашение между правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности : [заключено в г. Екатеринбурге 16.06.2009 г.] // Бюл. междунар. договоров. – 2012. – № 1. – С. 13–21.

33. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации : [заключено в г. Минске 01.06.2001 г.] // Содружество. – 2001. – № 1. – С. 138–145.

34. Устав Организации Объединенных Наций от 26 июня 1945 г. // Антология мировой политической мысли : в 5 т. / ред.-науч. совет:

Г.Ю. Семигин (пред.) [и др.]. – М. : Мысль, 1997. – Т. 5 : Политические документы / ред.-сост.: Ю.В. Ирхин [и др.]. – С. 343–392.

35. Факультативный протокол к Конвенции о правах ребенка, касающийся торговли детьми, детской проституции и детской порнографии от 25 мая 2000 г. : [подписан в г. Нью-Йорке 25.05.2000 г.] // Консультант Плюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО «Юр-Спектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2013.

Интернет-ресурсы

1. Организация Объединенных Наций [Электронный ресурс] / Организация Объединенных Наций. – Режим доступа: http://www.un.org/. – Дата доступа: 28.04.2019.

2. Комиссия международного права Организации Объединенных Наций [Электронный ресурс] / Организация Объединенных Наций. – Режим доступа: http://www.un.org/law/ilc/. – Дата доступа: 28.04.2019.

3. Аудиовизуальная библиотека материалов по международному праву [Электронный ресурс] / Организация Объединенных Наций. – Режим доступа: http://www.un.org/law/avl/. – Дата доступа: 28.04.2019.

4. Международный Суд Организации Объединенных Наций [Электронный ресурс] / Международный Суд ООН. – Режим доступа: http://www.icj-cij.org/. – Дата доступа: 28.04.2019.

5. Постоянная Палата третейского суда [Электронный ресурс] / Постоянная Палата третейского суда. – Режим доступа: http://www.pca-cpa.org/. - Дата доступа: 28.04.2019.

6. Европейский суд по правам человека [Электронный ресурс] / Совет Европы. – Режим доступа: http://www.echr.coe.int/. – Дата доступа: 28.04.2019.

7. Международные суды [Электронный ресурс] / Международные суды. – Режим доступа: http://www.worldcourts.com/. – Дата доступа: 28.04.2019.

8. Американское общество международного права [Электронный ресурс] / Ам. общ. межд. права. – Режим доступа: http://www.asil.org/. – Дата доступа: 28.04.2019.

9. Договоры, принятые в рамках Организации Объединенных Наций [Электронный ресурс] / Организация Объединенных Наций. – Режим доступа: http://treaties.un.org/. – Дата доступа: 28.04.2019.

10. Договоры, принятые в рамках Совета Европы [Электронный ресурс] / Совет Европы. – Режим доступа: http://conventions.coe.int/. - Дата доступа: 28.04.2019.

11. Международное право [Электронный ресурс] / Международное право. – Режим доступа: http://www.worldlii.org/. - Дата доступа: 28.04.2019.

12. Океаны и морское право [Электронный ресурс] / Организация Объединенных Наций. – Режим доступа: http://www.un.org/Depts/los/index.htm. – Дата доступа: 28.04.2019.

13. Европейский журнал международного права [Электронный ресурс] / Европейский журнал международного права. – Режим доступа: http://www.ejil.org/. - Дата доступа: 28.04.2019.

14. Британский ежегодник международного права [Электронный ресурс] / Британский ежегодник международного права. – Режим доступа: http://bybil.oxfordjournals.org/reports/most-read. – Дата доступа: 28.04.2019.

15. Материалы Международного уголовного суда [Электронный ресурс] / Международный уголовный суд. – Режим доступа: http://www.iccnow.org/. - Дата доступа: 28.04.2019.

16. Европейский Союз [Электронный ресурс] / Европейский Союз. – Режим доступа: http://www.europa.eu.int/. – Дата доступа: 28.04.2019.

17. Международный Комитет Красного Креста [Электронный ресурс] / Европейский Союз. – Режим доступа: http://www.icrc.org/. – Дата доступа: 28.04.2019.

18. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Режим доступа: http://www.pravo.by. – Дата доступа: 28.04.2019.

19. Электронная библиотека правовой литературы [Электронный ресурс] / Bookfi. – Режим доступа: http://en.bookfi.org/. – Дата доступа: 28.04.2019.

Перечень рекомендуемых средств диагностики и методика формирования итоговой оценки

Для контроля качества усвоения знаний студентами используются ***устная и письменная формы диагностики.***

К устной форме диагностики компетенций относятся:

– устный опрос;

– анализ кейсов.

К письменной форме диагностики компетенций относятся:

– тест;

– эссе;

– решение задач (анализ заданного кейса).

Для оценки результатов учебной деятельности могут быть использованы электронные платформы Moodle и GoogleClass.

Итоговая оценка формируется по следующим критериям.

При оценке за ответы на лекциях и семинарских занятиях (опрос) учитывается полнота ответа, наличие аргументов, ссылок на нормы действующих международных договоров, актов органов международных организаций, нормативные правовые акты, примеры из практики и т.д.

При оценке решения кейса необходимо учитывать: правильность толкования юридических терминов, знание норм действующего международного права и законодательства Республики Беларусь, вариативность предлагаемых ответов, аргументированность ответа.

При оценке решения задач требуется оценить правильность и полноту правовой квалификации определенной ситуации, обоснованность правовых аргументов, полноту исследования источников, подлежащих применению, наличие логичных выводов.

Оценка эссе формируется на основе следующих критериев: оригинальность (новизна) постановки проблемы и способа ее интерпретации/решения, самостоятельность и аргументированность суждений, грамотность и стиль изложения и т.д.

Оценка за выполнение теста формируется исходя из процента правильных ответов обучающегося, и выглядит следующим образом:

– 0-10% – 1;
– 11%-29% – 2;
– 30%-49% – 3;
– 50%-54% – 4;
– 55%-59% – 5;
– 60%-69% – 6;
– 70%-79% – 7;
– 80%-89% – 8;
– 90%-94% – 9;
– 95%-100% – 10.

При формировании итоговой оценки используется рейтинговая оценка знаний студента, дающая возможность проследить и оценить динамику процесса достижения целей обучения. Рейтинговая оценка предусматривает использование весовых коэффициентов для текущего контроля знаний и текущей аттестации студентов по дисциплине.

Формирование оценки за текущую успеваемость:

- ответы на семинарских занятиях – 60 %;
- написание эссе – 10 %;
- выполнение тестов – 30 %.

Рейтинговая оценка по дисциплине рассчитывается на основе оценки текущей успеваемости и оценки на зачете с учетом их весовых коэффициентов Вес оценки текущей успеваемости составляет 50 %, оценки на экзамене – 50 %.

Примерная тематика семинарских занятий

Семинар 1.

Тема 1. Теоретические основы международной информационной безопасности

Вопросы для обсуждения:

1. Понятие и сущность информационной безопасности.
2. Место принципов и норм, регулирующих вопросы обеспечения международной информационной безопасности в системе международного права.
3. Особенности международной информационной безопасности (субъекты и объекты).

Задания:

1. Дайте определения следующим понятиям:
- информационная безопасность;
- кибербезопасность;
- компьютерная безопасность;
- международная информационная безопасность;
- угроза информационной безопасности;
- информационная война;
- вмешательство во внутренние дела государства.

2. Составьте схему "Место международно-правовых принципов и норм, регулирующих обеспечение информационной безопасности, в системе международного права".

3. Определите специфику субъектов и объектов обеспечения информационной безопасности.

4. Какие нормативно-правовые акты, регулируют вопросы противодействия угрозам в информационной сфере в: Республике Беларусь, Российской Федерации, Украине, Казахстане, Австрии, Франции?

Семинар 2-4.

Тема 2. Угрозы международной информационной безопасности

Вопросы для обсуждения:

1. Деструктивное информационное воздействие и международное право.
2. Квалификация информационного воздействия в качестве вмешательства во внутренние дела государства.
3. Использование информационной инфраструктуры для распространения информации, разжигающей межнациональную, межрасовую и межконфессиональную вражду.

4. Пропаганда и международное право.

Задания:

1. Дайте определения следующим понятиям:
- информационная безопасность;
- международная информационная безопасность;
- угроза информационной безопасности;
- информационная война;
- вмешательство во внутренние дела государства.

2. Составьте схему "Международно-правовое регулирование нейтрализации угроз международной информационной безопасности".

3. Какие нормативно-правовые акты, регулируют вопросы противодействия угрозам в информационной сфере в: Республике Беларусь, Российской Федерации, Украине, Казахстане, Австрии, Франции?

Задачи:

1. На одном из российских каналов вышла передача новостей, в ходе которой сообщалось о невиданных зверствах, которые совершаются украинскими ополченцами на Донбасе. И в частности, приводился пример распятия ребенка на площади в одном из городов. Впоследствии выяснилось, что информация не соотвествует действительности.

1. Можно ли квалифицировать такие новости в качестве пропаганды? Почему?

2. Предусмотрена ли современным международным правом ответственность за распространение информации, которая не соответствует действительности?

3. Какие действия должны были быть предприняты телеканалом (государственными органами РФ) после того, как выяснилось, что сведения, приводимые в репортаже, не соответствуют действительности?

2. В Интернете появился блог, автор которого доказывал отсутствие факта Холокоста во времена Второй мировой войны. Автор блога являлся гражданином государства В. Гражданин А. обратился в правоохранительные органы государства Б и требовал принятия адекватных мер в отношении блоггера в связи с тем, что он глубоко оскорбил память погибших во времена Холокоста.

1. Является ли преступлением отрицание Холокоста? Почему?

2. Назовите международные договоры, запрещающие публикацию статей отрицающих/оправдывающих/поощряющих совершение преступлений против человечности и геноцида.

3. Если отрицание Холокоста является преступлением по законодательству государства Б, возможно ли привлечь блогера (гражданина государства А) к ответственности в государстве Б? Получить положи-

тельный ответ по запросу об экстрадиции блогера из государства А в государство Б?

Тестовые задания:

1. К преступлениям в сфере высоких технологий относится:

А. противоправный доступ к компьютерной информации;

Б. подкуп должностного лица, с целью внесения изменений в информацию, содержащуюся в компьютерной системе;

В. агрессия;

Г. воспрепятствование работе должностного лица, работающего с компьютерной информацией.

2. Специальные международные договоры в сфере обеспечения международной информационной безопасности заключены:

А. на универсальном, региональном и двустороннем уровне;

Б. на региональном и двустороннем уровне;

В. только на региональном уровне;

Г. только на универсальном уровне.

3. На основе какого из приведенных ниже принципов осуществляется взаимная правовая помощь по делам о преступлениях в сфере высоких технологий?

А. когнитивности;

Б. оперативности;

В. трансцендентности;

Г. атрибутивности.

4. Какие два основных вопроса регулирует Конвенция Совета Европы о киберпреступности:

А. гармонизация законодательства в уголовной сфере и оказание международно-правовой помощи

Б. унификация уголовного законодательства и регламентация права на доступ к информации

В. гармонизация законодательства в уголовной сфере и особенности обработки личных данных автоматизированными информационными системами;

Г. унификация уголовного законодательства и особенности обработки личных данных автоматизированными информационными системами.

5. В каких региональных международных организациях, координирующих международное сотрудничество в сфере обеспечения международной информационной безопасности, участвует Республика Беларусь:

А. ШОС;

Б. ОДКБ;

В. Совет Европы;

1. Что такое киберагрессия и кибертерроризм? Можно ли квалифицировать действия, указанные в задаче как киберагрессию или кибертерроризм?

2. С чем связаны «проблемы атрибутивности» совершенного деяния?

3. Должно (должны) ли нести международно-правовую ответственность государство (государства) в случае, если указанные действия совершены: а) хакерами на территории определенного государства; б) хакерами с территории нескольких государств; в) по заказу определенного государства; г) совершены сотрудниками специальных служб государства.

Семинар 6.

Тема 4. Роль международных организаций в обеспечении международной информационной безопасности

Вопросы для обсуждения:

1. Роль ООН в координации международного сотрудничества в области обеспечения международной информационной безопасности.

2. Деятельность Генеральной Ассамблеи ООН, Совета Безопасности ООН в сфере обеспечения международной информационной безопасности.

3. Деятельность группы правительственных экспертов для изучения потенциальных угроз в сфере информационной безопасности и возможных совместных мер по их устранению.

Задания:

1. Расшифруйте аббревиатуры (при наличии) и дайте краткую характеристику компетенции в сфере обеспечения информационной безопасности следующих органов международных организаций:

- Евроюст;
- ЕНИСА;
- Объединенный центр по компьютерным технологиям Интерпола;
- Отдел по финансовым преступлениям и преступлениям в сфере высоких технологий Интерпола;
- Рабочая группа по информационной безопасности ОДКБ;
- Центр передового опыта совместной киберзащиты НАТО;
- Центр по реагированию на киберугрозы НАТО.

2. Республика Беларусь является государством – членом СНГ и ОДКБ; Российская Федерация – СНГ, ОДКБ, ШОС, Совета Европы. Все указанные региональные международные организации в той или иной степени координируют сотрудничество государств в сфере обеспечения информационной безопасности. Выявите, имеются ли дублирующие функции в органах, созданных в этих организациях.

Задачи:

1. Хакерскую атаку, предпринятую весной 2017 г. на компьютерные системы по всему миру, Европол назвал нападением «небывалого масштаба». По последним данным, хакерскому нападению подверглись 75 тыс. компьютеров в примерно 100 странах по всему миру.

Так, например, больницы в Великобритании были вынуждены отправить многих пациентов домой. В субботу в Англии и Шотландии работа десятков медицинских учреждений была все еще парализована. Людей попросили обращаться за помощью только в самых неотложных случаях. Некоторые медучреждения из соображений безопасности отключили свои компьютеры[2].

1. Каковы правовые основы деятельности Европола? Можно ли сказать, что Европол является международной межправительственной организацией? Свое мнение аргументируйте.

2. Какова роль Европола в координации сотрудничества в борьбе с киберпреступностью? Какими полномочиями он обладает?

3. Какие органы Европейского союза будут координировать сотрудничество компетентных органов государств – членов ЕС в пресечении противоправной деятельности, указанной в задаче, если в ее результате начнут гибнуть пациенты больниц в Великобритании, ФРГ, Италии и Франции?

Семинар 7.

Тема 5. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий

Вопросы для обсуждения:

1. Формы и направления международно-правового сотрудничества в борьбе с преступностью в сфере высоких технологий.
2. Международное договорно-правовое регулирование сотрудничества государств в борьбе с преступностью в сфере высоких технологий на универсальном уровне.
3. Международное договорно-правовое регулирование сотрудничества государств в борьбе с преступностью в сфере высоких технологий на региональном уровне.
4. Международное сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках ООН.
5. Международное сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках Интерпола.
6. Международное сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках СНГ.

---

[2] Европол назвал глобальную хакерскую атаку беспрецедентной [Электронный ресурс] / Белорусский портал tut.by. – Режим доступа: https://news.tut.by/world/543147.html. – Дата доступа: 22.11.2018.

7. Международное сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках Совета Европы.

8. Международное сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках Европейского Союза.

9. Международное сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках ОДКБ.

Задания:

1. Покажите с помощью кругов Эйлера соотношение следующих понятий: 1) преступление в сфере компьютерной информации, преступление в сфере высоких технологий, киберпреступление; 2) преступление в сфере информационных технологий, киберпреступление, преступление в сфере высоких технологий.

2. Составьте таблицу «Договорно-правовое регулирование сотрудничества в борьбе с преступностью в сфере высоких технологий», в которой укажите действующие международные договоры, регулирующие сотрудничество государств в борьбе с преступностью в сфере высоких технологий; проекты таких договоров; международные организации под эгидой которых они заключены (под эгидой которых предполагается их заключить)

Задачи:

1. В многопользовательской онлайн игре «Мир танков» у одного из пользователей (гражданин Польши) «похитили» танк на сумму 100 долларов США. Злоумышленниками оказались граждане Беларуси.

1. Подпадают ли указанные действия под регулирование: а) Конвенции ООН против транснациональной организованной преступности; б) Конвенции Совета Европы о киберпреступности.

2. Могут ли быть привлечены к уголовной ответственности граждане Беларуси за приведенные в задаче действия? Приведите ссылки на уголовное законодательство Республики Беларусь.

2. В течение 5 лет с банковских счетов граждан США, ФРГ, Франции, Великобритании похищались денежные средства хакерами из Беларуси, Польши и Украины.

1. *Подпадают ли указанные действия под регулирование: а) Конвенции ООН против транснациональной организованной преступности; б) Конвенции Совета Европы о киберпреступности.*

2. Правоохранительные органы какого государства уполномочены проводить предварительное расследование и привлечение к уголовной ответственности в судебном порядке лиц, совершивших противоправные действия, указанные в задаче?

Описание инновационных подходов и методов к преподаванию учебной дисциплины (практико-ориентированный, метод анализа конкретных ситуаций, кейс-метод)

При организации образовательного процесса используется целый ряд методов, способствующих приобретению обучающимися социально-личностных, профессиональных и академических компетенций.

Практико-ориентированный подход, который предполагает:

- освоение содержание образования через решения практических задач;
- приобретение навыков эффективного выполнения разных видов профессиональной деятельности;
- ориентацию на генерирование идей, реализацию групповых студенческих проектов, развитие предпринимательской культуры;
- использованию процедур, способов оценивания, фиксирующих сформированность профессиональных компетенций.

Метод анализа конкретных ситуаций (кейс-метод),который предполагает:

- приобретениестудентом знаний и умений для решения практических задач;
- анализ ситуации, используя профессиональные знания, собственный опыт, дополнительную литературу и иные источники.

При организации образовательного процесса используется также **аналитический метод**,в котором нужно найти логическое решение ситуации по заданной фабуле. Ответ может быть изложен письменно (эссе). В процессе выполнения обучающиеся приобретают конкретный профессиональный опыт, развивают творческое мышление.

Методические рекомендации по организации самостоятельной работы обучающихся

Для самостоятельной работы используются следующие формы работы:

– поиск (подбор) и обзор литературы и электронных источников по индивидуально заданной проблеме курса;

– выполнение домашнего задания;

– решение задач и заданий, предусмотренных для семинарских занятий;

– изучение материала, вынесенного на самостоятельную проработку, подготовка по ним презентаций;

– анализ статистических и фактических материалов по заданной теме;

– подготовка и написание эссе.

Эссе должно составлять не более 4 страниц текста (размер шрифта 14pt, одинарный интервал), представлять собой самостоятельную работу студента, не содержать недобросовестных заимствований. При подготовке эссе в обязательном порядке должны выявляться и анализироваться нормативные правовые акты, решения международных судов и арбитражей, содержаться ссылки на позиции авторов.

В случае обнаружения любой доли плагиата работа оценивается отрицательно.

Примерная тематика реферативных работ (эссе)

1. Основные подходы к определению информационной безопасности.
2. Соотношение терминов «информационная безопасность», «кибербезопасность», «компьютерная безопасность».
3. Соотношение терминов «информационная безопасность» и «международная информационная безопасность».
4. Угрозы информационной безопасности.
5. Военно-политический подход к обеспечению информационной безопасности.
6. Юридическая квалификация кибер агрессии.
7. Юридическая квалификация кибертерроризма.
8. Правовые нормы, применимые к кибервойне.
9. Международно-правовая квалификация пропаганды.
10. Международно-правовая квалификация киберпреступлений.
11. Деяния с использованием информационных технологий, составляющие вмешательство во внутренние дела государства.
12. Применение силы и кибер атаки.
13. Международно-правовое сотрудничество в сфере обеспечения информационной безопасности.
14. Институциональные основы международного сотрудничества в области информационной безопасности.
15. Региональное сотрудничество в сфере обеспечения информационной безопасности.
16. Международно-правовое сотрудничество в борьбе с киберпреступностью.
17. Институциональные основы международного сотрудничества в борьбе с киберпреступностью.
18. Региональное сотрудничество в борьбе с киберпреступностью.
19. Взаимная правовая помощь по уголовным делам в цифровую эпоху.
20. Юрисдикция в киберпространстве.
21. Ответственное поведение государств в киберпространстве.
22. Применение принципа должной осмотрительность к деяниям в киберпространстве.
23. Обеспечение информационной безопасности и соблюдение прав человека.
24. На пути к универсальному договору об обеспечении информационной безопасности.
25. На пути к универсальному договору о борьбе с киберпреступностью.

Примерный перечень вопросов к зачёту

1. Понятие и сущность информационной безопасности. Особенности международной информационной безопасности (субъекты и объекты).
2. Основные направления обеспечения международной информационной безопасности.
3. Противодействие военно-политическим угрозам в сфере международной информационной безопасности.
4. Деструктивное информационное воздействие и международное право. Квалификация информационного воздействия в качестве вмешательства во внутренние дела государства.
5. Использование информационной инфраструктуры для распространения информации, разжигающей межнациональную, межрасовую и межконфессиональную вражду. Пропаганда войны.
6. Информационная война, информационное оружие и международное право.
7. Международное право, применимое к военным действиям в киберпространстве.
8. Особенности договорно-правого регулирования обеспечения международной информационной безопасности.
9. Региональные международные договоры, регулирующие сотрудничество государств в области информационной безопасности.
10. Роль мягкого права в регулировании обеспечения международной информационной безопасности.
11. Роль ООН в координации международного сотрудничества в области обеспечения международной информационной безопасности.
12. Деятельность региональных международных организаций в области обеспечения информационной безопасности (НАТО, ОДКБ, СНГ, ШОС).
13. Особенности правового регулирования обеспечения информационной безопасности в ЕС.
14. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий.
15. Формы и направления международно-правового сотрудничества в борьбе с преступностью в сфере высоких технологий.
16. Международное договорно-правовое регулирование сотрудничества государств в борьбе с преступностью в сфере высоких технологий.
17. Международное сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках международных организаций (ООН, Интерпол)
18. Международное сотрудничество в борьбе с преступностью в сфере высоких технологий в рамках региональных международных организаций.
19. Участие Республики Беларусь в международно-правовом сотрудничестве в области обеспечения информационной безопасности.
20. Участие Республики Беларусь в международно-правовом сотрудничестве в борьбе с преступностью в сфере высоких технологий.

ПРОТОКОЛ СОГЛАСОВАНИЯ УЧЕБНОЙ ПРОГРАММЫ

по факультативное дисциплине

«Международно-правовые основы информационной безопасности»

Название учебной дисциплины, с которой требуется согласование	Название кафедры	Предложения об изменениях в содержании учебной программы учреждения высшего образования по учебной дисциплине	Решение, принятое кафедрой, разработавшей учебную программу (с указанием даты и номера протокола)
Международное публичное право	Кафедра государственного управления	Нет предложений	Изменений не требуется. Протокол № 4 от 28 ноября 2019 г.

ДОПОЛНЕНИЯ И ИЗМЕНЕНИЯ К УЧЕБНОЙ ПРОГРАММЕ
по учебной дисциплине «Международное публичное право»
на _____/_____ учебный год

№№ пп	Дополнения и изменения	Основание

Учебная программа пересмотрена и одобрена на заседании кафедры государственного управления
(протокол № ____ от _____ 20_ г.)

Заведующий кафедрой
доктор юридических
наук, доцент _____ Т.А. Червякова
(степень, звание) (подпись) (И.О.Фамилия)

УТВЕРЖДАЮ
Декан факультета
доктор юридических
наук, профессор _____ С.А. Балашенко
(степень, звание) (подпись) (И.О.Фамилия)